NASA/CR-1999-209548

A System for Integrated Reliability and Safety Analyses

Peter Kostiuk and Gerald Shapiro
Logistics Management Institute, McLean, Virginia

Dave Hanson, Stephan Kolitz, Frank Leong, Gene Rosch, Marc Coumeri, and Peter Scheidler, Jr.
The Charles Stark Draper Laboratory, Cambridge, Massachusetts

Charles Bonesteel
Chava Group, Boston, Massachusetts

August 1999

NASA/CR-1999-209548

A System for Integrated Reliability and Safety Analysis

Peter Kostiuk and Gerald Shapiro
Logistics Management Institute, McLean, Virginia

Dave Hanson, Stephan Kolitz, Frank Leong, Gene Rosch, Marc Coumeri, and Peter Scheidler, Jr.
The Charles Stark Draper Laboratory, Cambridge, Massachusetts

Charles Bonesteel
Chava Group, Boston, Massachusetts

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

Prepared for Langley Research Center
under Contract NAS2-14361

August 1999

Available from:

NASA Center for AeroSpace Information (CASI)
7121 Standard Drive
Hanover, MD 21076-1320
(301) 621-0390

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161-2171
(703) 605-6000

Contents

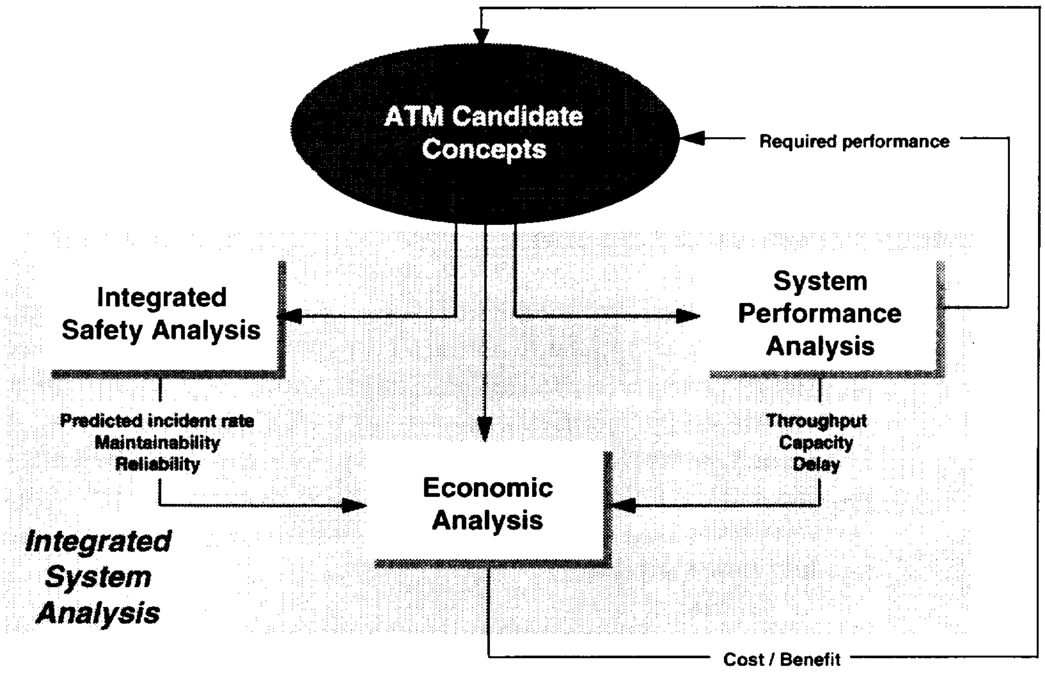
FIGURES

TABLES

Problem Definition

In this program, we have continued the development of an integrated systems analysis methodology for analyzing innovation in Air Traffic Management (ATM).[1] This methodology, illustrated in Figure 1, integrates safety analysis, operational performance analysis, and economic cost/benefit analysis. When new ATM developments are proposed, this methodology can be used to assess and balance their overall impact on the system from both economic and safety perspectives. The complexity of the trade-offs required can only be adequately addressed by using integrated analytical techniques of this kind.

Figure 1. Integrated Systems Analysis



The methodology we have developed is ideally suited to the kinds of analysis required by the new national aviation safety initiative, announced by Vice President Gore early in 1997. The goal of this initiative is to increase civil aviation safety by a factor of five over the next decade. The use of the civil aviation system is expected to increase significantly over the next decade, thus technology applied to increase the economic efficiency of civil aviation must simultaneously increase safety by an even greater factor. Since investment is required to achieve

[1] The development of this methodology has been the goal of several earlier programs in which we have participated [19], [20].

both objectives, a new level of scrutiny will be required from the analytical tradeoff studies that support the decision to apply any new technology.

The proposed implementation of the Wide Area Augmentation System (WAAS) adjunct to the existing Global Positioning System (GPS) is a prime example of a new technological application to the ATM system whose true economic value can only be assessed in the light of the new national aviation safety goals by using the type of integrated systems analysis methodology we have developed. The primary goal of WAAS is to increase the number of commercially useful runways throughout the United States (and the world). If safety were not an issue, WAAS would only have to prove itself to be an economically favorable alternative to installing more existing-technology precision approach systems (e.g., Instrument Landing Systems (ILS)) in order to justify its incorporation into the civil aviation system. It is likely that WAAS would, in fact, compare favorably in such a tradeoff. Unfortunately, some of the very characteristics that make WAAS economically desirable could potentially contribute to an increase in the absolute rate of approach accidents.[2] Thus, to assess its ultimate appropriateness as a new approach system, a new analysis tool will be required. In this program we have developed major portions of such a tool.

Operational Benefits of Wide Area Augmentation System

WAAS is an outgrowth of the Local Area Augmentation System (LAAS), currently under development to provide Category I approaches to all otherwise appropriately configured runways at a *single* airport. WAAS has the potential to provide the same capability to almost *all* such airports throughout the United States (and the world). Both WAAS and LAAS augment raw GPS information to provide sufficient three-dimensional position accuracy to approaching aircraft to permit them to land safely in weather conditions as poor as a 200-foot ceiling and one-half mile visibility.

After initial certification of Category I approaches for WAAS-equipped aircraft, it is planned to extend the new capability to Category II and Category III approaches, eventually permitting safe landings for appropriately equipped aircraft in zero-zero weather conditions at virtually all commercially significant airports. It may also be possible, using the Automatic Dependent Surveillance Broadcast (ADS-B) system currently under development, for appropriately-equipped aircraft to relay their WAAS-determined positions to Air Traffic Control (ATC) controllers on the ground, or to other aircraft, in real time, thus providing an attractive adjunct to, if not a substitute for, conventional surveillance radar systems. If operationally successful, all of these capabilities will move the civil aviation system

[2] In this report, the term absolute accident rate refers to the total number of system-wide accidents per unit time (e.g., total number of accidents per year). Relative accident rate refers to accidents per operation (e.g., accidents per flight-hour, accidents per passenger-mile, or accidents per approach).

significantly closer to the day when Free Flight, or the ability to operate safely in any weather conditions without constraints from ground controllers, can be achieved.

In addition to offering improved operational reliability to runways with existing Category I approach systems, WAAS offers a very low incremental cost alternative to providing new Category I capability to runways not currently served by ILS systems. Any airport not adversely masked from GPS signal reception by intervening terrain is a candidate for a WAAS Category I approach. If safety were not an issue, the benefit of such a system to civil aviation would be self-evident.

Safety, however, is very much an issue. Precisely because of its ability to open up large numbers of runways to Category I operations, the implementation of WAAS will significantly increase the exposure to the hazards inherent in these operations.

POTENTIAL HAZARDS OF WAAS

As potentially beneficial to future operations as WAAS may be, if the relative accident rate attributable to Category I approaches using WAAS were only to be equal to that currently attributable to similar approaches using ILS, then its net benefit to civil aviation would be questionable. Even if the relative approach accident rate remained constant, the dramatic increase in actual Category I approaches that WAAS would make possible would result in a net increase in the absolute accident rate in Category I weather conditions. If approach accidents were only a very small fraction of all accidents, then this might still conform to the new national aviation safety goal if other accident causes were reduced enough to compensate for the approach accidents. Unfortunately, this does not appear to be the case. Ten-year world-wide aviation accident statistics clearly show that the primary cause of all serious large aircraft accidents is Controlled Flight Into Terrain (CFIT), and that, of all such accidents, a significant portion occur during approaches in Instrument Flight Rule (IFR) conditions. Close scrutiny of these statistics, however, does suggest a steady and encouraging improvement in the situation, at least in the United States (the same trend is not as evident in non-U.S. accident statistics). One identifiable contributor to this improvement is the now-widespread use of Ground Proximity Warning Systems (GPWS) in large commercial aircraft (required for U.S.-certified carriers).

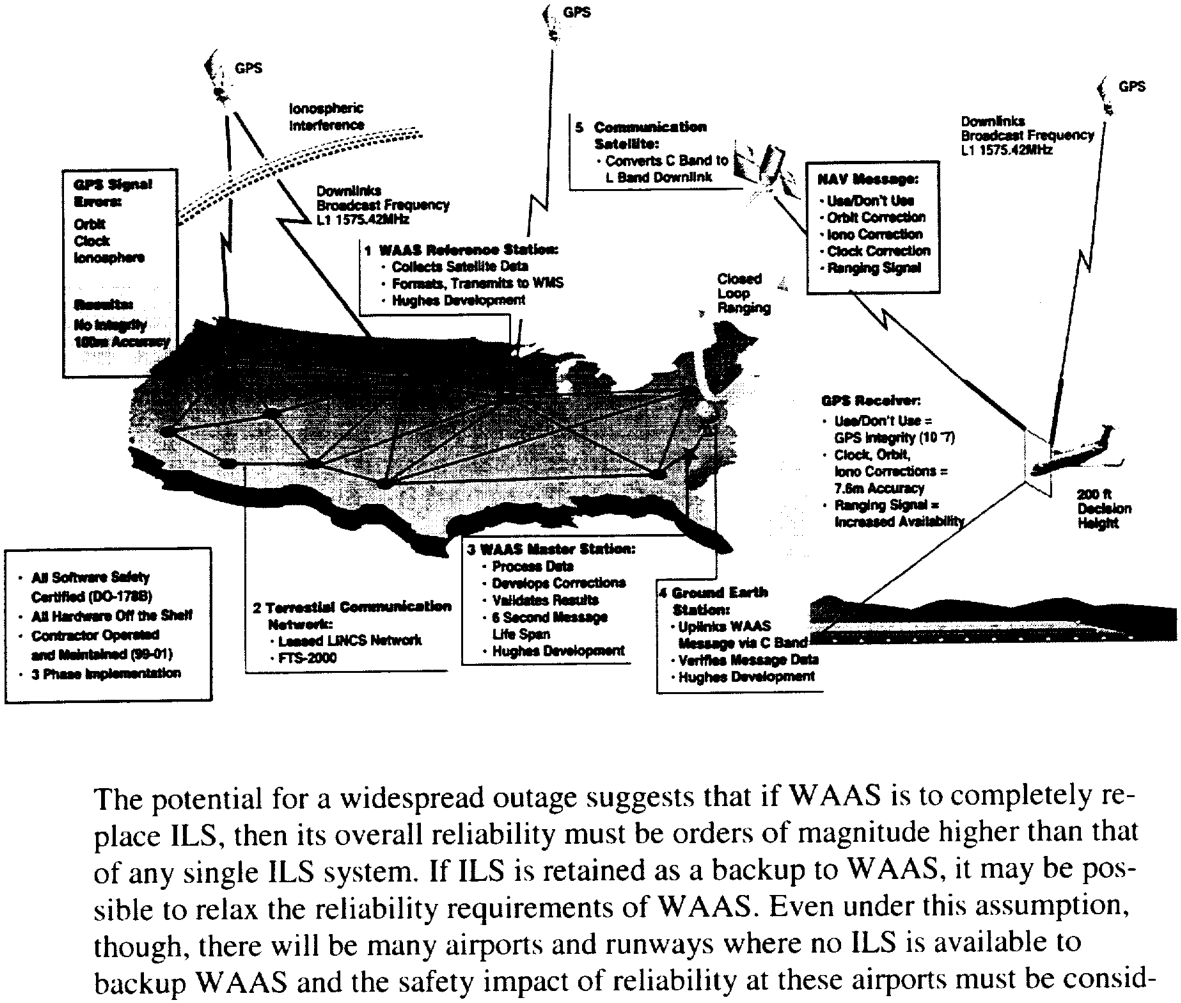
Nevertheless, the currently available statistics do not demonstrate that GPWS alone is enough to meet the national aviation safety goal. Thus it appears at least highly desirable, if not essential, that, when WAAS becomes operational, it must be significantly safer than ILS is today.

Hazards Attributable to WAAS Reliability

In addition to the safety impact due to increased exposure to Category I operations that WAAS will make possible, the hazard rate attributable to system reliability must be assessed.

WAAS is a complex system that augments GPS by the addition of numerous ground relay stations, ground-based processing centers, and up-links to dedicated communications satellites (Figure 2). To use the WAAS signals, aircraft must be equipped with appropriate GPS receivers, special processors and cockpit display systems. All of these elements of the system are subject to failure. Depending on where in the WAAS system a failure occurs, Category I approach capability may only be lost to a single aircraft operating at a single airport or simultaneously to all aircraft operating at all airports within a large geographic area.

Figure 2. WAAS Overview



The potential for a widespread outage suggests that if WAAS is to completely replace ILS, then its overall reliability must be orders of magnitude higher than that of any single ILS system. If ILS is retained as a backup to WAAS, it may be possible to relax the reliability requirements of WAAS. Even under this assumption, though, there will be many airports and runways where no ILS is available to backup WAAS and the safety impact of reliability at these airports must be considered when assessing the net benefit of WAAS to the entire civil aviation system.

There are also hazards associated with ADS-B. Should ADS-B be used in lieu of conventional surveillance radar to provide position information to other aircraft or ATC controllers, then, upon loss of certain WAAS or ADS-B components, the associated surveillance information would also be lost. Although the ATC system can function safely without direct surveillance information (provided that reliable air-to-ground communications remain available), it does so only with greatly reduced throughput. If it were relied upon as a primary source of surveillance data, the sudden loss of ADS-B capability during periods of high traffic density in Category I weather conditions would almost certainly create a hazardous transient environment.

The potential hazards just described are entirely dependent on the hardware and software reliabilities of the systems involved. To perform trade-off studies to optimize the use of WAAS, while conforming to the national aviation safety goals, requires tools to determine the reliability of these systems in various configurations and under various hypothetical scenarios. In this program, we have developed prototype reliability tools to perform such trade-off studies.

Hazards Attributable to Human Factors In The Use of WAAS

In addition to reliability-associated hazards, hazards attributable to the behavior of aircrews and ATC controllers are of major concern in safety analysis. Today, human factors are cited as a major or contributing cause in the majority of all aviation accidents. This is not to suggest that the humans involved are negligent in their behavior. By any standard, accidents in aviation are rare when compared with those of competing modes of transportation, and aviation accidents whose primary cause is human error are even more rare. Nevertheless, even highly skilled and well-trained humans make occasional mistakes. In order to meet the demanding goals of the national aviation safety initiative the system must become even more tolerant of human error than it is now.

Ergonomics is an increasingly significant aspect of modern aircraft design, and today's state-of-the-art aircraft are more tolerant of human error than ever before. When new equipment (e.g., complex, multi-function, integrated autopilots, flight directors, and flight control systems) is introduced, however, new levels of ergonomic consideration are often required. Digital technology is replacing analog technology at a phenomenal rate and the majority of humans—experienced pilots included—often find themselves in an unfamiliar environment that can lead to so-called mode confusion when operating complex systems. Unfortunately, ergonomic flaws that can lead to mode confusion and similar hazards do not become evident until *after* an accident has occurred. This method of diagnosing ergonomic flaws must be eliminated in order to meet the new national safety goals.

When poor ergonomic design can be eliminated as a contributing cause of an accident attributable to human behavior, we must focus on procedural inadequacies. Because of the complexity of some aircraft operations, their execution is often codified in the form of procedures to be followed almost by rote. Usually such procedures are more or less fail-safe, but circumstances can occasionally occur that were not anticipated by the procedure designers. One might call such an occurrence a procedural trap, or, more colloquially, a catch–22. If the national safety goals are to be met, existing and newly proposed operational procedures must be subject to higher levels of scrutiny than ever before.

Confining our focus to human factors during Category I approaches, several aspects of the system-wide problem become highlighted. Both ATC controllers and pilots are involved in the execution of approaches. The controllers must meter arriving aircraft so that they arrive at the appropriate initial approach fixes at rates that both maximize throughput while assuring no conflicts as the aircraft continue to execute their approaches. Once cleared for their approaches, pilots must manage their aircraft to assure stability of the approach, make proper decisions upon reaching decision height, and transition to safe landings or to appropriate missed approach procedures. These human skills are required for any kind of Category I approach, whether utilizing WAAS or ILS. Since WAAS will result in a significant increase in the number of Category I operations, human behavior in the use of WAAS will become even more significant than it was when only ILS systems were available.

Because of its substantial impact on relative accident rates, human behavior must become an integral part of the new level of analysis required to make the new national aviation safety goal a reality. Tools must become available which incorporate accurate models of human behavior in a wide variety of environments as an intrinsic part of their analytic structure. Our models incorporate the possibility for human error as a function of the operational environment.

Hazards Attributable to Increased Category I Exposure Due To WAAS

WAAS will make Category I operations possible at many airports and to many runways where such operations are not currently possible. Even if WAAS proves to be sufficiently reliable and tolerant of human error, the mere fact that very many more Category I approaches will be conducted, many of them to airports and runways where no such approaches have been possible in the past, will result in some accidents that would never have occurred without WAAS. Only if the rate of occurrence of these new types of accidents is *much lower* than the rate of increase in the corresponding new types of approaches will the introduction of WAAS be consistent with the new national aviation safety goals.

WAAS will provide the independent source of three dimensional position accuracy required for Category I approaches at any airport not adversely masked from GPS signals by local terrain (and the vast majority of commercially useful airports are not so masked). There is, in fact, no way to *prevent* the WAAS signals from being present at any such airport. These signals will be available to any aircraft with even marginally adequate WAAS equipment attempting to approach such airports at any time, regardless of runway length, local obstructions, supplemental systems such as approach lights, an outer marker (OM), a middle marker (MM), or even the presence of an ATC Tower[3]. In addition, although the aircraft involved must have some necessary minimum level of WAAS equipment installed, it is likely that the spectrum of equipment sophistication, air crew skills, training and experience will be much broader for operations at new WAAS Category I sites than it is today where only ILS systems are present. The net result will be that, although all else may be equal, there will likely be more Category I approaches taking place under circumstances much closer to minimally acceptable safety margins than there are today.

To assess the net impact on absolute safety that these WAAS-induced operational trends are likely to cause, only an appropriately faithful dynamic simulation of Category I operations can offer the required quantitative answers. This simulation must rely on hardware and software reliability analyses such as those discussed above and on human factors issues. LMI is currently developing such a simulation. When combined into the integrated systems analysis methodology described above, this combination of tools, research, and simulation promises to provide the required answers.

OPERATIONAL BENEFITS VERSUS POTENTIAL HAZARDS OF WAAS

The simplistic solution to the likely trend towards more Category I operations under near–minimum acceptable conditions would be to simply raise the minimum acceptable standards (e.g., by requiring more expensive equipment, more redundancy, larger flight crews, or higher flight times to qualify for advanced IFR ratings, etc.). This, however, would adversely affect the increased throughput of the civil aviation system that WAAS itself is intended to facilitate. In the limit, if the simplistic approach were adopted, the minimum acceptable standards might have to be raised so high that, in order to meet them (and, thereby, meet the national safety goals) the system throughput would be held to current levels, or even less than current levels. A complex paradox suggests itself: must operational functionality be *decreased* in order to *increase* absolute safety levels? This is not an easy question to answer. Defeatist hyperbole asserts that to minimize aviation accidents, airplanes should never be allowed to leave the ground. The obvious, but much more difficult, alternative is to develop the system so that, without unduly raising its minimum acceptable operational standards (and, perhaps, even lowering them), its intrinsic accident rates are made to become acceptably low. If WAAS is to truly contribute to the national safety goals, then it must *both* increase system throughput *and* increase absolute system safety. To determine if it

[3] Category I approaches are currently authorized at numerous airports without ATC Towers, or at airports where such towers only operate part-time, but the number of such airports will likely increase significantly with the introduction of WAAS.

can do so requires assessing the reliability, human factors, and operational issues that will result from the introduction of WAAS.

These considerations bring us back to the initial premises of this section of this report: 1) the new national aviation safety initiative requires an order of magnitude improvement in relative accident rates; 2) to meet these goals, a corresponding increase in the level of aviation safety analysis capability is required; and 3) our accomplishments in this project, as discussed in the remainder of this report, contribute directly to that end.

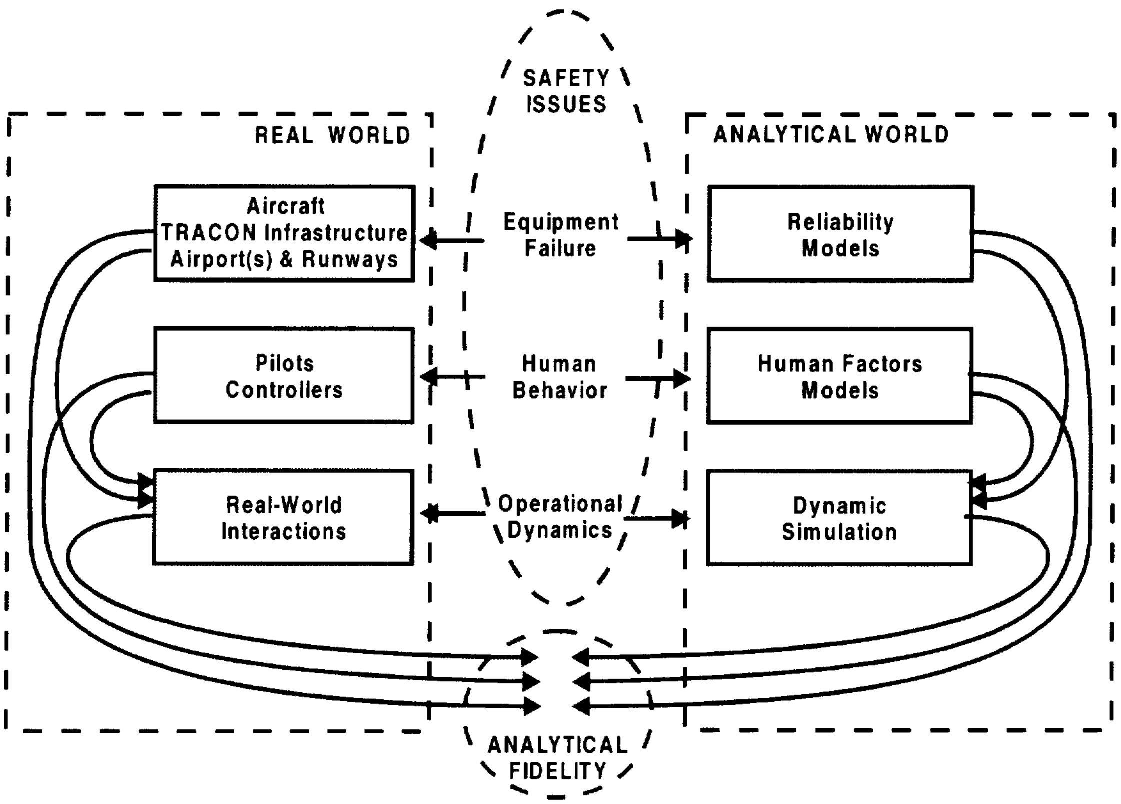
Approach

The preceding section has defined the problem in terms that require an integrated systems analysis methodology in which three well-defined activities must take place: 1) development of reliability tools capable of easily assessing a wide variety of new technologies in a wide variety of new and existing operational environments; 2) human factors research to determine the impact of human behavior on aircraft and ATC operations; and 3) incorporation of these analytic elements into a dynamic operational simulation.

Our approach to implementing this methodology is to develop an Integrated Systems Analysis Tool (ISAT) with three major parts, each related to one of the three major safety issues described above. This approach is illustrated in Figure 3.

Figure 3 contrasts the real world of ATM with the parallel analytical world of our methodology as implemented in ISAT. In the real world equipment degrades and fails. In ISAT we employ reliability models to gain quantitative insight into those degradations and failures. In the real world pilots and controllers occasionally operate at less than ideal performance levels. In ISAT the human factors research we have initiated will lead to models providing quantitative insights into degraded human behavior, similar to those that the reliability models provide for degraded equipment operation. Finally, in the real world, both equipment and humans interact with complex operating environments (which include both air traffic dynamics and weather influences) in ways that occasionally result in hazardous situations. In ISAT the data generated by the reliability and human factors models will drive the dynamic simulation to assess, in quantitative terms, the overall impact of these hazardous situations on air traffic throughput and safety.

Figure 3. Relationship Of Integrated Systems Analysis Methodology To Aviation Safety Issues

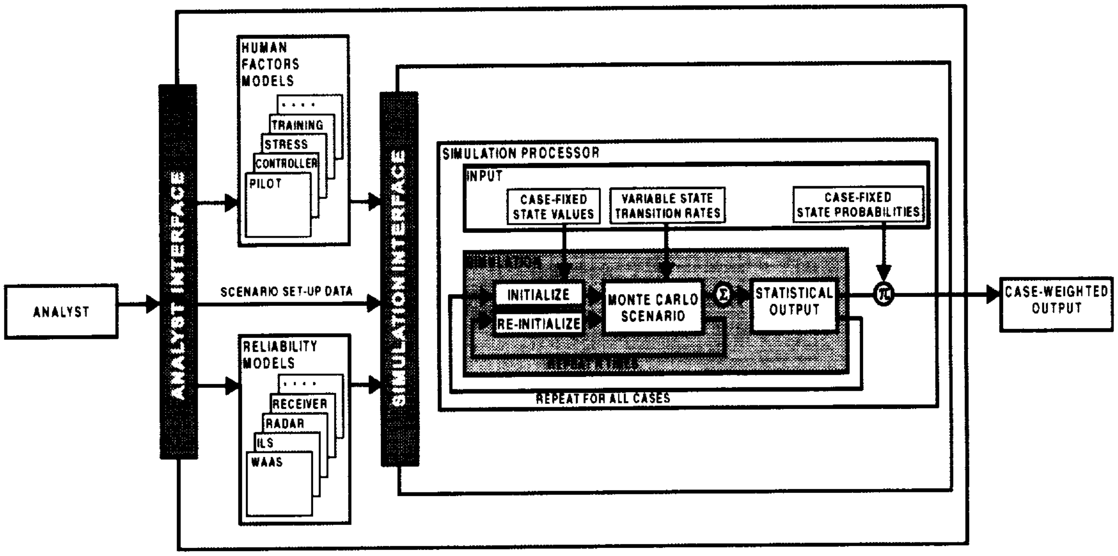


The converging arrows that are encircled and identified as analytical fidelity at the bottom of Figure 3 imply that the validity of the quantitative insights generated by ISAT are only as sound as its component models are faithful to their counterparts in the real world. In the previous project [20], we validated a model similar to the one being developed in this project with real experimental data. On the basis of that validation, we believe that our integrated systems analysis methodology for analyzing innovation in ATM is sound. In this project, we have made significant advancements towards the goal of implementing that methodology through an ISAT, which will support the level of aviation safety analysis required in the future.

THE INTEGRATED SYSTEMS ANALYSIS TOOL (ISAT)

Figure 4 is a top-level conceptual block diagram of the ISAT. When complete, this tool will consist of three major components: reliability tools, human factors tools, and a dynamic air traffic simulation. In addition there will be two major interfaces: a front-end analyst interface, and an internal simulation interface. An analyst will formulate the scenarios he or she wishes to examine via the user interface, configure the reliability and human factors tools to generate the data required by the simulation, and run the simulation through various numbers of cases in order to generate safety and throughput data from which analytical conclusions can be drawn.

Figure 4. Integrated Systems Analysis Tool



Uncertainty and Stochastic Analysis

An important issue in performing any analytical investigation using the methodology we have been developing is the determination of the best way to characterize uncertainty in the analysis. In the air traffic system there is always some uncertainty in such operational parameters as aircraft position and speed, time lags between cause and effect events, human reaction times, etc. The weather itself varies with varying degrees of unpredictability; ceilings float up and down over some range, visibility fluctuates and sometimes changes suddenly, icing conditions change, and so on. These uncertainties are commonplace and, although most of the time they do not lead to hazardous situations, they have an effect upon operations and must be part of any analysis involving safety issues. They are most appropriately modeled as random fluctuations within the dynamic simulation itself. There is, in fact, no other mathematically tractable way to consider them.

Many of the uncertainties associated with safety analysis are far more rare than the type of natural noise just described. Critical electronic equipment, for example, is designed to be very reliable. Since the simulation will model a period of an hour or so at most, whereas the mean time between failures for this type of critical equipment is typically at least several thousand times larger, randomly generating the occurrence of such failures would require an inordinately large number of iterations to achieve acceptable statistical confidence. Instead, low-probability-of-occurrence events critical to aviation safety need to be modeled explicitly and the results weighted by the associated probabilities of their occurrence. For example, it is clear that the worst time for a WAAS failure would be when an arriving aircraft is approaching decision height in solid IFR conditions. Such an event is far too rare to even consider evaluating in a random process, yet, it is possible, and, if it did lead to an accident, the resulting consequences could be extremely severe. Instead of treating such an incident as a random event which may or may not occur in any given system simulation run, two (or more) comparative cases could be run using the ISAT, both with random simulation of the common natural uncertainties described above. In one of these cases, the WAAS would never fail, and in the other it would always fail[4]. Since the probability of WAAS failure is known from the reliability models, the results of both cases can be compared analytically.

In Figure 4, the two methods for characterizing stochastic events in the ISAT are depicted, conceptually, within the box labeled simulation processor. Here, the common uncertainties are shown as a loop within the simulation itself. For any given run of the simulation this loop will be iterated as many times as necessary to achieve the required statistical confidence. The output of a given run of the simulation will be statistical in nature (e.g., data will be expressed as means and variances of the output variables of interest). The rare events will be run on a case by case basis, each case constituting a separate run of the simulation with its Monte Carlo processes fully exercised each time. Each of these rare cases will have an associated probability of occurrence derived from the reliability or human factors tools. The statistical output data from each run of the simulation will then be appropriately weighted in a post-processor to derive final results.

Reliability Tools

Integrated systems analysis in general, as exemplified by our analysis of WAAS, requires the ability to assess the reliability of complex systems associated with the ATM system with ease and accuracy. When new systems are proposed, their future reliability must be predicted and compared with the existing systems. For analyzing WAAS, the reliability of a minimum of the following three systems must be assessed:

1. WAAS itself (including both the signal-generation system and the aircraft equipment which must receive and process those signals);
2. the existing ILS system; and
3. existing surveillance radar (whose function may be augmented or replaced by the use of ADS-B in association with WAAS).

[4] The precise timing of the failure relative to the time at which any given aircraft will reach decision height will, in effect, be the result of other random processes in the simulation. Since the precise moment at which any given aircraft will reach decision height will fluctuate from one iteration of the model to another, a WAAS failure that is triggered to occur at a specific time will occur with some variable time relative to decision height time. This characterization is desirable because it will tend to smooth out apparent dependencies on irrelevant parameters.

Numerous computer programs have been developed to assess the reliability of complex physical systems. A number of these have been developed by government agencies, including NASA. Rather than new development, we chose to incorporate existing NASA reliability tools into the ISAT. Because these tools must function as part of a larger, all-inclusive integrated systems analysis methodology, however, we concluded that, in the ISAT, tool initialization must be isolated from the detailed operation of the tools themselves to the maximum extent possible. Our goal has been to allow the analyst to be free to concentrate on the big picture aspects of the problem without having to be distracted by the details of operating the component tools themselves. To that end, we have developed a preliminary user interface that facilitates input to the NASA reliability models. In the final ISAT, this interface will be part of the analyst interface shown in Figure 4.

Reliability models that have been developed are discussed in detail in the section Reliability Modeling and Analysis.

Simulation Interface

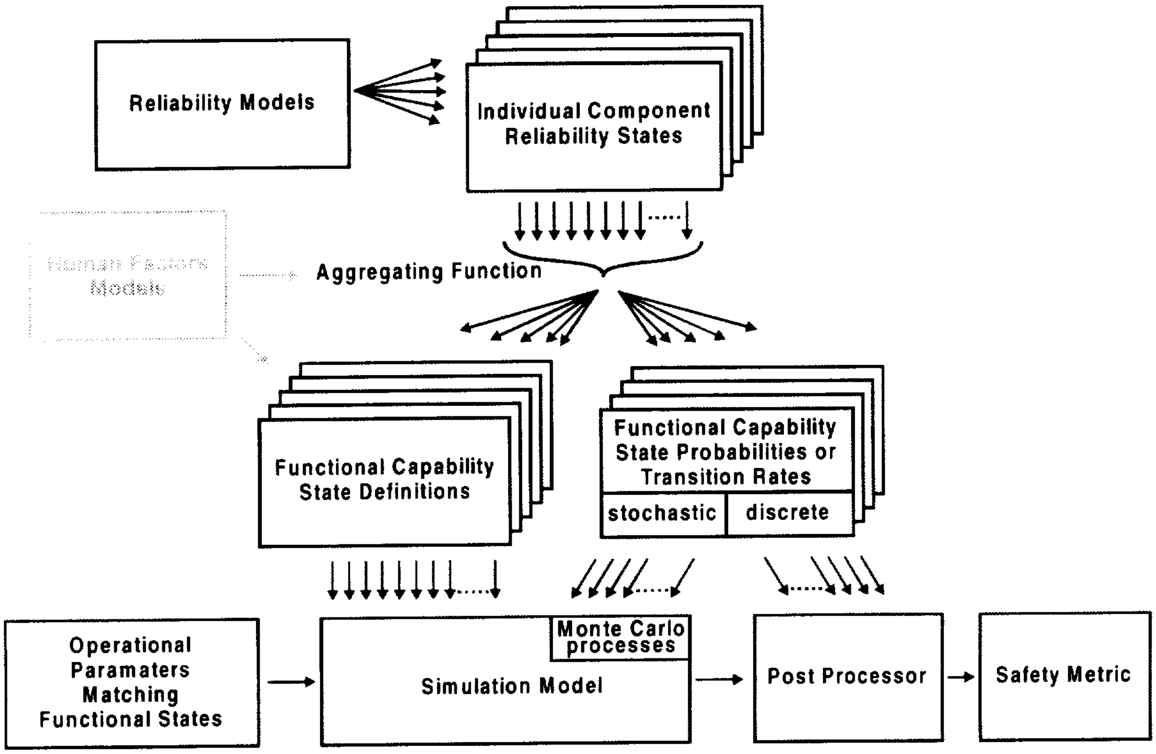
As a result of applying the reliability tools to new and existing hardware and software items used in the air traffic system, the analyst can calculate the probability that any given item will be in any one of a number of operational capability states. If the object is fully functional, as it was designed to be, then its performance can be expected to be normal and the simulation will model that item using a set of normal characterizing parameters. If it is in some degraded state of functionality, then its performance can be expected to be abnormal in some way and the simulation will replace its normal parameter set with one of the degraded parameter sets. The possible states and the associated sets of characterizing parameters for each item will be inputs to the simulation. When a state transition occurs, the simulation will simply switch from the parameter set associated with the state before the transition to that associated with the state after the transition. Thus the impact of the abnormal performance of any item in the system can be assessed in the dynamic context of the entire system. Our task is to assure that all of the information required to perform the assessment is available to the simulation. In the ISAT, this is provided by the internal simulation interface shown in Figure 4. The simulation model itself is described in Appendix A.

The dynamic system simulation will model a large number of aircraft (on the order of a few hundred) arriving and departing from a major airport within a TRACON over a period of an hour or so. It has appropriate characterizations of pilots and controllers exchanging information over a communications system. It will accommodate normal and abnormal performance in all pertinent objects, including aircraft, navigation and approach aids, ground facilities, and the airport(s) and runways. Each of these objects may be in one of several well defined capability states ranging from fully functional to completely inoperative, including distinguishing between inoperability states where the failure is known to the system operators (failed safe) and states where the failure is undetected. Some state changes can occur within the model, either as a result of deterministic logic or by a random (Monte Carlo) process. Other states will remain fixed throughout a given execution of the model.

The simulation is both object oriented and event sequenced. When events occur, objects perform various actions. The action performed by any given object upon the occurrence of any given event is determined by the state of that object. We have developed state spaces for the three object classes most directly associated with efficient and safe air traffic operations within a TRACON: the TRACON itself (a class of one), the aircraft (a class containing as many objects as there are aircraft to be simulated), and the environment (i.e., weather) (also a class of one).

The possible states for each class of objects can be very large and is most conveniently defined by arranging them in a logical hierarchy. Various combinations of the large number of possible states that result can be aggregated into overall functional capability states for objects in the simulation. Thus, for example, a given aircraft may be classed as operating normally if all of its component objects are operating normally. The aircraft may be operating in a moderately degraded mode if certain combinations of its components are degraded. In general various different combinations of component degradation may all result in the same overall level of degradation for the aircraft. In principal, then, for any object, the number of operational functionality states will be much smaller than the number of all possible combinations of component object degradations. This process of aggregating individual component states into overall operational functionality states is illustrated in Figure 5.

Figure 5. Aggregating Component Reliability States into Functional Capability States


Reliability Models
Individual Component Reliability States
Human Factors Models
Aggregating Function
Functional Capability State Definitions
Functional Capability State Probabilities or Transition Rates
stochastic
discrete
Operational Paramaters Matching Functional States
Monte Carlo processes
Simulation Model
Post Processor
Safety Metric

TRACON STATES

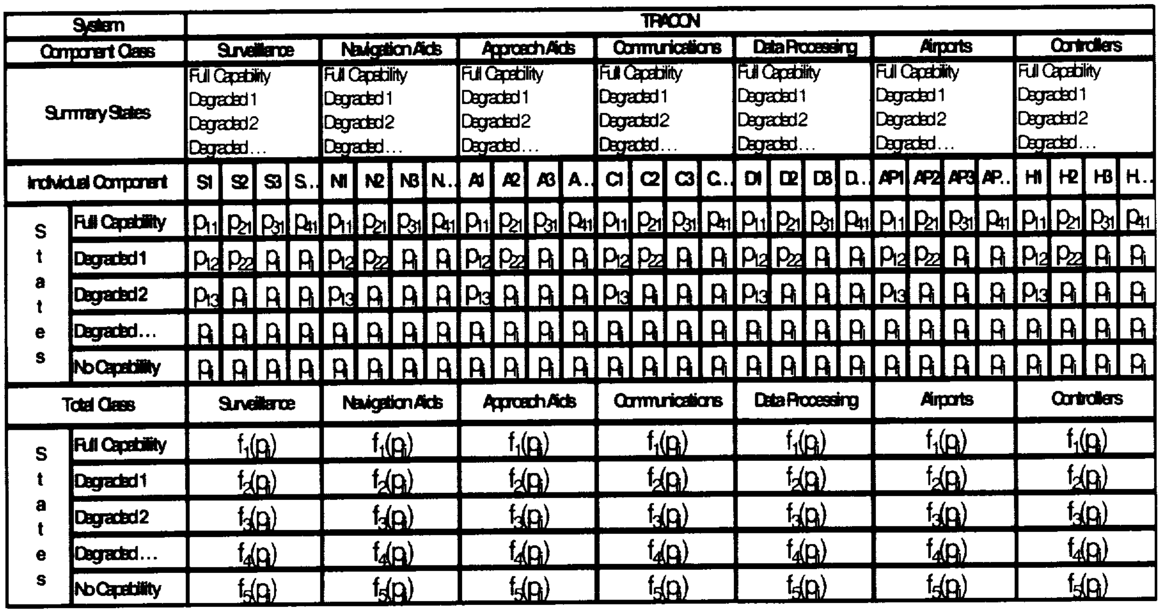
A typical TRACON consists of a variety of constituent objects that interact with arriving and departing aircraft to achieve the goal of efficient and safe air traffic operations. As shown in Figure 6, the TRACON objects can be categorized roughly into seven sub-classes based on the function that they perform: 1) surveillance systems; 2) navigation aids; 3) approach aids; 4) communications systems; 5) data processing systems; 6) airports[5]; and 7) controllers. Figure 7 shows, conceptually, how the operability states of various objects within each of these categories can be combined to define an overall level of functionality for each of the functions that these seven categories of objects implement.

[5] Although TRACONs are established to handle arrival and departure traffic for specific major airports, most also have jurisdiction over numerous smaller airports within their geographical boundaries. A few have jurisdiction over more than one major airport.

Figure 6. TRACON Object Hierarchy

Object Class	Function ~ Object sub-class	Functional components ~ Objects	Purpose of Function performed by Object (component)
TRACON	Surveillance	Local Radars	Provide TRACON controllers with position and altitude information for ALL aircraft within the TRACON boundaries
		Center Radars	
		ADS-B	
		Pilot Position Reports	
	Navigation	VORs	Provide aircraft (pilots) with position information with sufficient accuracy to reach their initial approach fix (arrivals) or TRACON exit points (departures)
		VORTACs	
		NDBs	
		GPS	
		Radar Fixes	
	Approach	ILS Localizers	Provide aircraft (pilots) with position and altitude information with sufficient accuracy to land safely in current weather conditions
		ILS Glideslopes	
		OMs	
		MMs	
		IMs	
		Approach lights	
		Threshold lights	
		Centerline lights	
		WAAS	
		LAAS	
	Communications	Ground-to-air radios	Enable communications between TRACON controllers and pilots, Center controllers, or airport Tower controllers
		Ground-to-ground links	
	Data Processing	Computers	Process air traffic control data for display to, and use by, TRACON controllers
		Displays	
		I/O Consoles	
	Airports	Runways	Provide arrival (landing) and departure (takeoff) facilities for aircraft
		Towers	
	Controllers	Controllers	Manage air traffic

Figure 7. TRACON Capability State Hierarchy



System		TRACON																											
Component Class		Surveillance				Navigation Aids				Approach Aids				Communications				Data Processing				Airports				Controllers			
Summary States		Full Capability Degraded 1 Degraded 2 Degraded...				Full Capability Degraded 1 Degraded 2 Degraded...				Full Capability Degraded 1 Degraded 2 Degraded...				Full Capability Degraded 1 Degraded 2 Degraded...				Full Capability Degraded 1 Degraded 2 Degraded...				Full Capability Degraded 1 Degraded 2 Degraded...				Full Capability Degraded 1 Degraded 2 Degraded...			
Individual Component		S1	S2	S3	S..	N1	N2	N3	N..	A1	A2	A3	A..	C1	C2	C3	C..	D1	D2	D3	D..	AP1	AP2	AP3	AP..	H1	H2	H3	H..
States	Full Capability	P_{11}	P_{21}	P_{31}	P_{41}	P_{11}	P_{21}	P_{31}	P_{41}	P_{11}	P_{21}	P_{31}	P_{41}	P_{11}	P_{21}	P_{31}	P_{41}	P_{11}	P_{21}	P_{31}	P_{41}	P_{11}	P_{21}	P_{31}	P_{41}	P_{11}	P_{21}	P_{31}	P_{41}
	Degraded 1	P_{12}	P_{22}	P_{ij}	P_{ij}	P_{12}	P_{22}	P_{ij}	P_{ij}	P_{12}	P_{22}	P_{ij}	P_{ij}	P_{12}	P_{22}	P_{ij}	P_{ij}	P_{12}	P_{22}	P_{ij}	P_{ij}	P_{12}	P_{22}	P_{ij}	P_{ij}	P_{12}	P_{22}	P_{ij}	P_{ij}
	Degraded 2	P_{13}	P_{ij}	P_{ij}	P_{ij}	P_{13}	P_{ij}	P_{ij}	P_{ij}	P_{13}	P_{ij}	P_{ij}	P_{ij}	P_{13}	P_{ij}	P_{ij}	P_{ij}	P_{13}	P_{ij}	P_{ij}	P_{ij}	P_{13}	P_{ij}	P_{ij}	P_{ij}	P_{13}	P_{ij}	P_{ij}	P_{ij}
	Degraded...	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}
	No Capability	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}	P_{ij}
Total Class		Surveillance				Navigation Aids				Approach Aids				Communications				Data Processing				Airports				Controllers			
States	Full Capability	$f_1(P_{ij})$				$f_1(P_{ij})$				$f_1(P_{ij})$				$f_1(P_{ij})$				$f_1(P_{ij})$				$f_1(P_{ij})$				$f_1(P_{ij})$			
	Degraded 1	$f_2(P_{ij})$				$f_2(P_{ij})$				$f_2(P_{ij})$				$f_2(P_{ij})$				$f_2(P_{ij})$				$f_2(P_{ij})$				$f_2(P_{ij})$			
	Degraded 2	$f_3(P_{ij})$				$f_3(P_{ij})$				$f_3(P_{ij})$				$f_3(P_{ij})$				$f_3(P_{ij})$				$f_3(P_{ij})$				$f_3(P_{ij})$			
	Degraded...	$f_4(P_{ij})$				$f_4(P_{ij})$				$f_4(P_{ij})$				$f_4(P_{ij})$				$f_4(P_{ij})$				$f_4(P_{ij})$				$f_4(P_{ij})$			
	No Capability	$f_5(P_{ij})$				$f_5(P_{ij})$				$f_5(P_{ij})$				$f_5(P_{ij})$				$f_5(P_{ij})$				$f_5(P_{ij})$				$f_5(P_{ij})$			

In the surveillance category, for example, a typical TRACON will employ some number of radar, most equipped with secondary (transponder) radar, as their primary surveillance sensors. Other sensors might also be available, either as primary or back-up data sources (including, possibly, ADS-B with WAAS-derived data). Each of these devices has various failure modes. Depending on the particular failure modes, and the availability of back-up systems, the many possible combinations of individual equipment failure states can be mapped into a much smaller overall operational functionality state for the surveillance function itself. This is indicated, on Figure 7, by the column of notional probabilities, P_{ij}, for each device i, being in capability state j, within the surveillance category. These probabilities, in turn, map into similar capability states for the entire surveillance function. In the model, operations that depend on surveillance will behave differently depending upon the overall surveillance capability state. The capability states of the other TRACON functions will be structured similarly. The final category of TRACON objects includes the key TRACON controllers. The Human Factors models will define these states and their probabilities.

Aircraft States

Whereas the simulation will use only one TRACON object, there will typically be several hundred aircraft operating within the TRACON. As shown in Figure 8, each aircraft will be modeled as an object belonging to a class of Aircraft Objects, consisting of six functional object sub-classes: control, navigation, approach, communication, situation awareness, and crew. Although its specifics are different, the method of combining, or aggregating individual component object states into an overall capability state for the corresponding aircraft function is similar to that described above for component TRACON objects.

Figure 8. Aircraft Object Hierarchy

Object Class	Function ~ Object sub-class	Functional components ~ Objects	Purpose of Function performed by Object (component)
AIRCRAFT	Control	Engines Control Surfaces Landing Gear Control Linkage Cockpit Controls Flight Directors	Provide the ability for the pilot to cause the aircraft to follow a desired flight path
	Navigation	VOR/VORTAC Receivers NDB Receivers GPS Receivers Directional Systems	Provide position information to the pilot with sufficient accuracy to follow a flight plan or respond to a new clearance
	Approach	ILS Receiver ILS Processor & Display WAAS Receiver WAAS Processor & Display	Provide position information to the pilot with sufficient accuracy to reach decision height safely in any weather conditions
	Communication	Ground-to-air radios	Enable communications between pilots and ground controllers
	Situation Awareness	Maps and charts Outside visibility Crew experience "Mental picture"	Enable crew to adequately perceive the position And circumstances of their aircraft with respect to the truth
	Crew	Crew	Operate the controls and execute the decisions necessary to conduct the required flight operations

ENVIRONMENTAL STATES

By far the most significant factor affecting aviation safety is the weather. In the simulation, the environment will be an object class of its own, as illustrated in Figure 9. Environmental object sub-classes are defined so as to interact with the dynamic air traffic as directly as possible. They include five object categories: time of day, ceiling, visibility, flight rules, and weather.

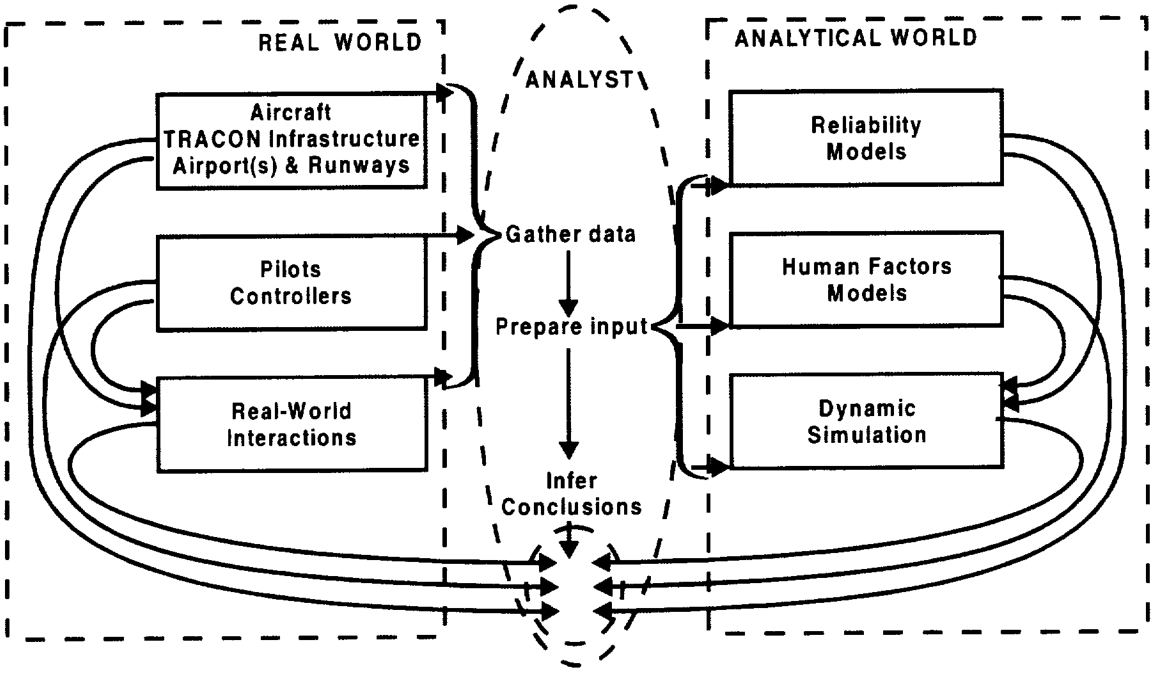
Figure 9. Environment Object Hierarchy

Object Class	Function ~ Object sub-class	Functional Components ~ Objects	Purpose of Function Performed By Object (Component)
Environment	Time of Day	Day Night	Set illumination level
	Ceiling	Ceiling	Establish altitude from which aircraft crews can see the ground beneath them
	Visibility	Visibility	Establish horizontal distance from which aircraft crews can see objects when beneath the ceiling
	Flight Rules	Instrument Flight Rules (IFR) Visual Flight Rules (VFR)	Establish required air traffic control procedures, crew qualifications and aircraft equipment
	Weather	Wind Precipitation	Establish wind conditions (calm...gusty...sheer...turbulence...thunderstorm) Establish precipitation (none...rain...snow...hail...icing conditions)

USING THE ISAT

Use of the ISAT parallels its development. Each part of the ISAT reflects a major portion of the air traffic system and must be initialized to reflect the real world situation that the analyst wishes to examine. This process is illustrated in Figure 10.

Figure 10. Using the Integrated Systems Analysis Methodology



Suppose an analyst would like to compare the safety consequences of WAAS and ILS failures occurring just prior to a specific aircraft reaching decision height during a CAT I approach. The baseline scenario might simulate normal operation in a TRACON for a 30-minute period, then trigger an ILS glideslope failure during the next approach to occur. The analyst would set up the scenario with ILS only and have all common stochastic processes selected for simulation as Monte Carlo processes during each run. The rest of the states would be set to fixed values for each run and would not change during that run. The first case would run enough Monte Carlo iterations to achieve necessary statistical confidence, and *in all iterations* the glideslope for a given runway would fail shortly after 30 simulated minutes into the run. For the second case, the analyst would remove the ILS system from the runway in question and implement simulation of WAAS. All other input parameters would remain unchanged. Associated with each case would be a probability of failure determined by the reliability model, in the first case, the probability of ILS glideslope failure and, in the second, the probability of WAAS failure. The model would measure the safety impact on the overall system in each case and might report such parameters as the average number of hazardous incidents occurring before and after the failure. Presumably the number of such incidents before the failure would be the same for both cases; however, the number after the failure might differ. The relative merit of each system could be assessed by multiplying the respective changes in hazardous incidents by the relative probabilities of each type of system failing.

RELIABILITY MODELING AND ANALYSIS

In this section, we discuss several reliability modeling techniques and present Markov reliability models of: (1) a surveillance radar system, (2) an ILS approach system and (3) the Wide Area Augmentation System (WAAS).

Reliability Modeling Techniques

Three classes of standard reliability modeling techniques are simulation, combinatorial models, and Markov modeling.

Using simulation (e.g., Monte Carlo simulation), system reliability is determined by generating failure and repair events at times distributed according to the component failure and repair rates. Simulations are repeated until statistically significant reliability measures are accumulated. A major strength is the ability to analyze complicated repair and reconfiguration scenarios. A disadvantage is that for highly reliable systems, the failure rate is so low that a very large number of simulations must be run to accumulate a statistically meaningful number of events.

Combinatorial models (e.g., Fault-Tree Analysis) are based on a system architecture and redundancy management approach, in which component failure probabilities are combined to determine system reliability. One limitation of this approach is the difficulty of including events that have order dependencies, (e.g. repairs and reconfiguration strategies). Also, because all combinations of events for the entire time period must be included, this approach can result in a complicated fault tree that is difficult to construct and validate.

Markov modeling techniques calculate the probability of the system being in its various **states** as a function of time. A state represents the system status with respect to component failures and the behavior of the system's redundancy management strategy. Transitions from one state to another occur at given transition rates that reflect component failure and repair rates and redundancy management performance. Advantages of Markov modeling include: (1) model construction does not require *explicit* generation of all possible combinations of events that can occur over the entire time period; (2) order dependent events are included naturally; and (3) the model is solved analytically (or numerically), avoiding simulation. A disadvantage is that the state space can grow exponentially with the number of components. However, in many situations of interest techniques have been developed to render this problem tractable, including model truncation, state aggregation, and behavioral decomposition.

From a reliability point of view, the real-world radar and ILS systems are far too complex to be analyzed in detail within the scope of this task. Instead, in order to illustrate the methodology involved, we selectively grouped areas of detail into aggregates that can be characterized in our models as single objects.

Having aggregated the details into manageable groups, we define exactly what happens to the overall system when one or more of those aggregated groups fail, either totally, or partially. These are the formal failure modes of the system.

The next step is to define the failure modes as states. This is the first point in the process where mathematical rigor must be strictly imposed. Some general comments of Markov processes are in order before proceeding.

The states of the system must be well defined and complete, in the sense that the system is always in one of the states. Since the system can change states at random intervals, there is a probability associated with finding the system in any given state at some arbitrary time. The sum of these probabilities over all states must equal 1.0 (another way of saying that the set of states is complete). When the system changes from one state to another, we say that it transitions from the previous state to the new state. To satisfy the mathematical requirements of a Markov process, the probability that the system can transition from any one of its states to any other state must not depend on past history, but only on the two states involved (the previous state and the new state). Finally, a stationary Markov process is one in which the transition probabilities do not change with time.

Discrete Markov processes only can make transitions from one state to another at discretely specified intervals. They are completely defined if all of the transition probabilities are defined. Differential Markov processes can change states at any time. For these, instead of defining a transition probability, we define a transition rate. Its units are transitions per unit time (whereas transition probabilities are just dimensionless numbers).

Reliability models of complex systems can be fit into the mathematical mold of differential Markov processes. In such models, each state of the system represents one of the ways in which some aggregated set of its components can fail. In redundant systems, some failures will not change the overall functionality of the system, some failures will result in degraded functionality, and some failures will result in no functionality or overall system failure. One of the states is the no-failure state. We can think of the system as starting out in its no-failure state. The rate at which it will transition from no-failure to another state is the aggregate failure rate of the components that define the new state.

Reliability models also include repairs. Given that the system is in one of its failed states, it can return to the no failure state at a rate equal to the repair rate (in units of repairs per unit time) for the aggregated components.

Given the states, the next step in the process is to define precisely exactly what can happen in the real world to force the system to transition from one state into another. This step is complete when a Markov transition matrix can be defined, at least symbolically.

Data specifying the quantitative failure rates or mean times between failures for each aggregate of components must be obtained by actual observation, by experiment, by off-line simulation, or by exercising good engineering judgment.

Since we are interested in levels of operational functionality, there will be, in general, several Markov states that, collectively, result in the same level of functionality (to the level of detail that is important to our problem). These must be identified so that we can sum their probabilities of occurrence to determine the desired probabilities of having a given level of functionality.

The ASSIST [1] and PAWS [2] reliability programs were used to generate and solve the system architecture descriptions described in this report. Both of these reliability programs come from a NASA reliability program tool chest.

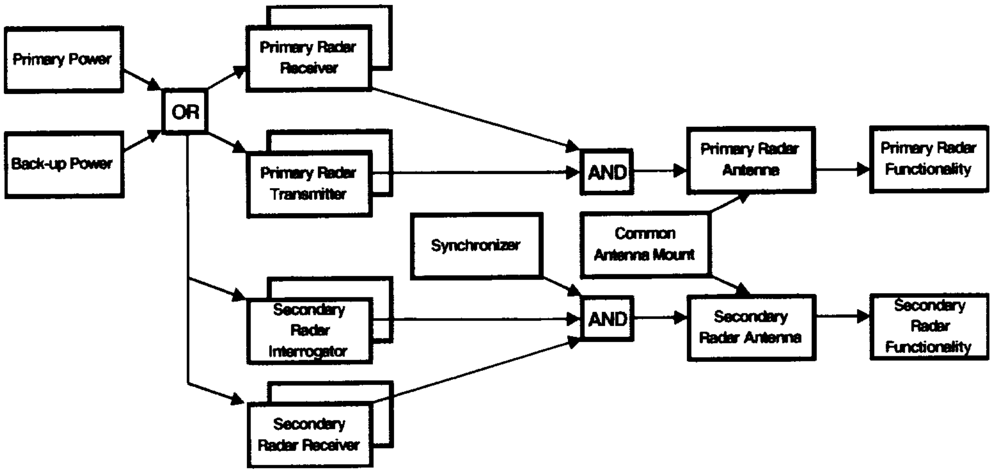
The ASSIST program (Abstract Semi-Markov Specification Interface Tool) provides a flexible, user-friendly interface for the textual description of the system's architecture. The ASSIST program builds the model by recursively applying the transition rules that are defined for the architecture. This Markov model description may then be used within the PAWS reliability analysis program.

The PAWS (Pade Approximation With Scaling) program calculates the state probabilities at a given mission time. A wrapper routine (TARAT [3]) iterates through the subsystems and combines the results, yielding the overall functional modes.

Surveillance Radar Reliability Model

Figure 11 is a simplified top-level diagram of a surveillance radar system. This is a generic diagram representing a system with dual redundant-critical components. The system includes both a primary radar that can track the skin return from any target in its coverage area and a secondary radar, or beacon system, which sends out interrogations that trigger transponder responses in all transponder-equipped aircraft. The primary radar has dual redundant transmitters and receivers, and the secondary radar has dual redundant interrogators and receivers.

Figure 11. Surveillance Radar Reliability Model



The primary and secondary antennas are rigidly connected, and share a common rotating antenna mount. Secondary (beacon) radar interrogations are synchronized to the pulses transmitted by the primary radar. The system is assumed to have both primary and backup power sources.

For this system, it is assumed that a single failure in any transmitter, interrogator, or receiver leaves the overall system functional. A second failure in one of those components, however, results in the loss of the associated functionality (i.e., either the primary or secondary radar functionality is lost). Either power source can fail without bringing the system down; however, if both fail, the entire system is lost. If the common antenna mount fails, the antennas cannot rotate and the entire system is lost. Finally, if the secondary radar synchronizer fails, secondary radar functionality is lost.

Appendix B displays the ASSIST file used to define the system architecture for the primary radar architecture. A total of 31 states were generated for the primary radar model.

Appendix C displays the ASSIST file used to define the system architecture for the secondary radar architecture. A total of 67 states were generated for the secondary radar model.

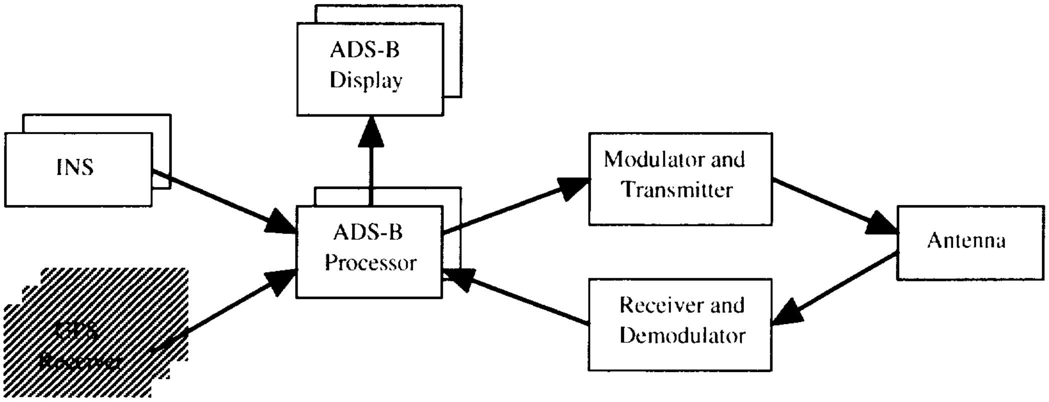
Appendix D displays the ASSIST file used to define the system architecture for the common radar architecture components (the common antenna mount along with the primary and backup power source). A total of 12 states were generated for the common radar model.

ADS-B/Surveillance Data Link Reliability Model

The ADS-B/Surveillance Data Link is onboard each equipped aircraft. It transmits the position estimate of the aircraft and receives the position estimate broadcast from other ADS-B equipped aircraft. The position broadcast from the aircraft allows other ADS-B equipped aircraft within range of the broadcast to monitor its position. Similarly, the ADS-B position estimates received from other aircraft provide greater situational awareness to the crew and aid in avoiding collisions with other ADS-B equipped aircraft.

Different aircraft could be equipped with different ADS-B equipment of differing designs and reliabilities. Figure 12 shows the design that is modeled in the current safety tool. The GPS Receivers and INS (Inertial Navigation Systems) provide the sensor data that the ADS-B Processor uses to generate the position estimate of the aircraft. The ADS-B Processor broadcasts this position via the Modulator and Transmitter and Antenna. The ADS-B Processor receives position estimates from other ADS-B equipped aircraft via the Antenna and Receiver and Demodulator. The ADS-B Processor presents the location of these aircraft to the crew on the ADS-B Display.

Figure 12. ADS-B/Surveillance Data Link



The duplicate blocks in Figure 12 indicate the redundancy of each type of component. Specifically, there are 2 redundant INS, 3 redundant GPS Receivers, 2 redundant ADS-B Processors, and 2 redundant ADS-B Displays. (The broken lines shown for the GPS Receivers indicate the GPS Receivers are not included in the ADS-B/Surveillance Data Link function because they are included in the WAAS GPS Receiver function.) Arrows indicate the connections between the components. Connected components are fully cross-strapped. For example, the connection between the GPS Receivers and the Processors indicated by the arrow means each of the 3 GPS Receivers is connected to each of the Processors.

The ADS-B/Surveillance Data Link function is defined to have three states: Fully Operational, Failed Safe, and Failed Uncovered. For the ADS-B/Surveillance Data Link function to be Fully Operational, 1 INS, 1 ADS-B Processor, 1 ADS-B Display, the Modulator and Transmitter, the Receiver and Demodulator, and the Antenna must be functional. The ADS-B/Surveillance Data Link function remains

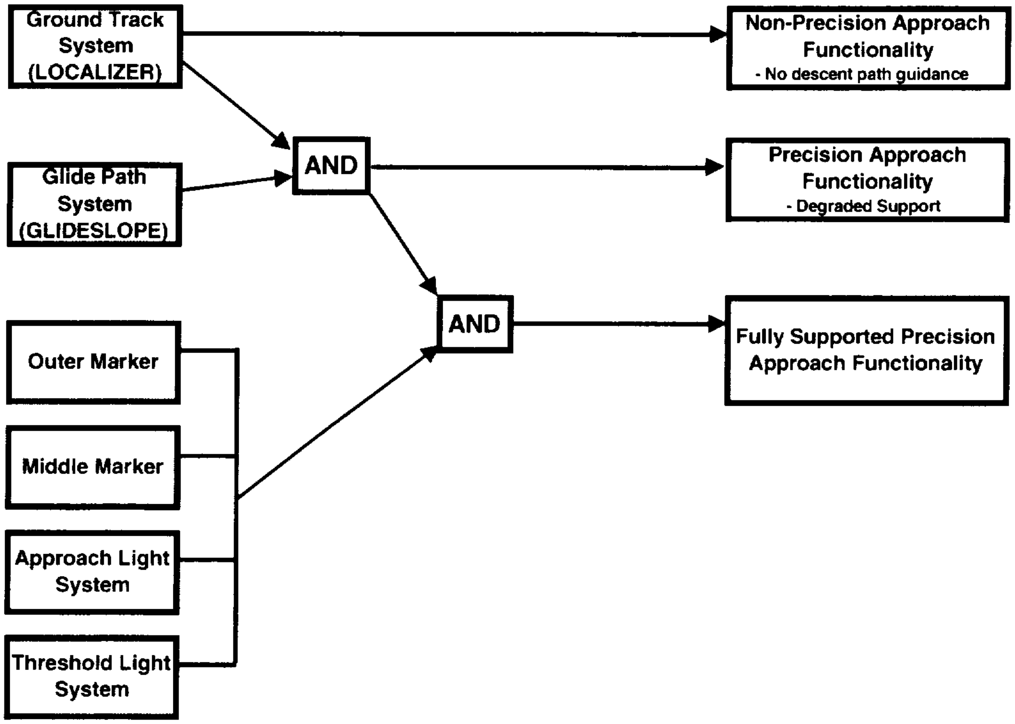
Fully Operational as failures occur as long as the Failure Detection, Isolation and Reconfiguration (FDIR) process successfully detects and removes component failures. The Failed Safe state results if the FDIR process successfully detects and removes a component failure, but the minimum number of components of each type are no longer functional. If this occurs, the ADS-B/Surveillance Data Link provides an alert to the crew. If a failure of a component should occur and the FDIR process does not detect and remove it, this results in the Failed Uncovered state.

The Markov model for the ADS-B/Surveillance Data Link function provides the probability of being in each of the function states for the time period the aircraft is in the TRACON air space. Appendix E presents the ASSIST input file used to generate the Markov model for the ADS-B/Surveillance Data Link function.

Precision Approach System Instrument Landing System Reliability Model

Figure 13 is a simplified top-level diagram of a precision approach system. It is modeled after a standard system, but it is sufficiently generic to represent any system that provides independent guidance in both the vertical and horizontal planes to aircraft approaching to land. The system consists of two major subsystems, the ground track system (or, in the case of an ILS system, the localizer) and the glide path system (or glideslope). In addition, it is supported by independent outer and middle markers (for systems utilizing an inner marker it would also be included in the support systems) and approach and threshold lighting systems.

Figure 13. Instrument Landing System Reliability Model


Ground Track System (LOCALIZER)
Glide Path System (GLIDESLOPE)
Outer Marker
Middle Marker
Approach Light System
Threshold Light System
AND
AND
Non-Precision Approach Functionality
- No descent path guidance
Precision Approach Functionality
- Degraded Support
Fully Supported Precision Approach Functionality

This reliability model incorporates the ability to alter the repair strategy. If, for example, the glideslope were to fail, TRACON could elect to shut down the approach and have it repaired immediately, thereby taking the associated runway out of service. Alternatively, they could continue to operate with the localizer only, delaying the repair until a future time. This reliability model enables a user to select repair strategies for all components except the localizer.

To accommodate the variable repair strategies two states are assigned to each failure (other than the localizer). These are "wait to start repair" and "start repair immediately." If the "wait" strategy is selected, then a mean wait time is introduced and an additional transition is required before the repair can begin. If the "repair immediately" strategy is selected, the waiting state is skipped and the system goes directly into repair.

Appendices F and G display the ASSIST files used to define the radar architecture. Appendix F is for the "wait" strategy; Appendix G is for the "repair immediately" strategy.

WAAS

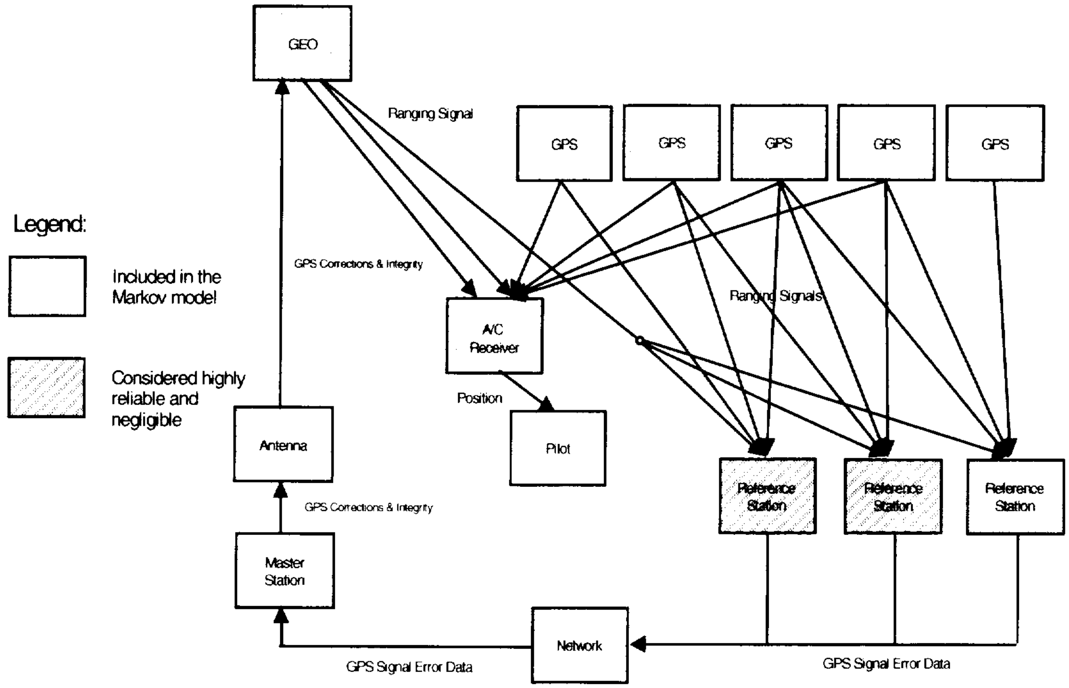
System Description

GPS system limitations include insufficient integrity, availability, and accuracy. Integrity is the ability of the system to provide timely warnings to users when the system should not be used for navigation. GPS integrity notification time is 15 minutes or greater, which is not sufficient for civil aviation. Availability is the percentage of time that services of the system are usable. GPS system availability of all 24 satellites is 70 percent and availability of at least 21 satellites is 98 percent. Availability of 99.999 percent is desired for systems used as the primary means of navigation. Accuracy is the degree of conformance of the estimated position to the true position. The GPS satellite signal includes errors due to the orbit, clock, and ionosphere. GPS accuracy for civilian use is 100 meters. This accuracy is acceptable for en route through non-precision approach, but is not acceptable for precision approaches. Hence, GPS does not satisfy civil aviation requirements for usage as the primary means of navigation.

The Wide Area Augmentation System, WAAS, augments the position measurements of the Global Position System, GPS, by providing additional ranging signals, position corrections, and integrity monitoring. When processed by the WAAS-GPS receiver, the system will attain integrity of 10^{-7}, 7.6 m accuracy, and increased availability. WAAS is available throughout the continental United States. Aircraft equipped with WAAS-GPS receivers can use WAAS as the primary means of navigation, with sufficient integrity, availability, and accuracy for the 200-foot decision height required on CAT I precision approach landings.

Figure 14 is a simple block diagram illustrating the major components of WAAS and their interdependence. The GPS and geosynchronous communication satellites broadcast position-ranging signals, which are received by numerous WAAS reference stations distributed throughout the continent. These reference stations transmit the GPS signal error data via a ground network to the WAAS master stations. Each master station processes the GPS signal error data yielding GPS corrections and integrity which is uplinked to the geosynchronous communication satellites via an antenna. The geosynchronous communication satellite broadcasts the GPS corrections and integrity in addition to the ranging signal. The aircraft's WAAS-GPS receiver receives and processes both ranging signals from the GPS and geosynchronous communication satellites, as well as the GPS corrections and integrity signals from the geosynchronous communication satellites. The receiver processes these signals resulting in an accurate and reliable position measurement which is displayed for the pilot to read. (Components highlighted in dark gray were included in the Markov model; other components were considered highly reliable and therefore negligible.)

Figure 14. WAAS System Analysis



There are 24 GPS satellites; however, at any instant in time in the TRACON area, only 4 to 13 are in range. There are 4 geosynchronous communication satellites, plus one on-orbit spare. No more than two of these geosynchronous communication satellites are in view at any time. The spare may be called into action if another geosynchronous communication satellite fails. Current plans for WAAS include 35 or more reference stations distributed throughout the continental United States and Canada. Current WAAS implementation also calls for at least two master stations, one on each coast. Two to three ground-earth stations, or uplink antennas, are available near each master station. Table 1 summarizes this information.

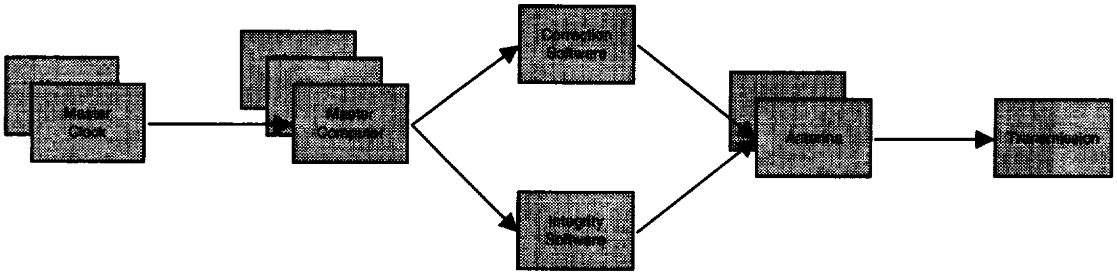
Table 1. WAAS Physical Components

Component	Total Number	Number TRACON	Failure Modes
GPS Satellites	24	4 to 13	2
GEO Communication Satellites	5 (4+ spare)	1 to 2 + spare	2
Reference Stations	35+	Many	0
Ground Network	1	1	0
Master Station	2+	1 to 2	4 to 5
Ground Earth Station (Antenna) per station – GEO satellite link	2 or 3	2 to 3	2
WAAS/GPS Receivers per aircraft	2 to 3	2 to 3	4
Pilots per aircraft	1 to 2	1 to 2	?

The WAAS failure modes were identified from system specifications and engineering judgement. The FAA WAAS specifications define two failure modes each for the GPS and geosynchronous communication satellites, long-term and short-term. Long-term failure represents a catastrophic failure, requiring launch of a replacement satellite. Short-term failure represents a temporary failure, requiring re-initialization of satellite systems and software. Reference stations individually have several failure modes, but there is a very high level of redundancy. Hence, assuming there are no common failure modes (e.g., a common software bug), no failure modes were modeled. Likewise, the ground network is also highly reliable and therefore no failure modes were modeled.

The master station includes numerous components (Figure 15) for which 5 failure modes have been identified. The master station has a master clock, master computer with hardware, operating system, and software. Failure modes based on FAA specifications define the operating system failure mode repair and partially define software failure modes. Additional master station failure modes are based on engineering judgement. Two failure modes were modeled for the software, one each for the position correction and integrity monitoring software. Each antenna was assumed to have two failure modes, representing hardware and transmission failures.

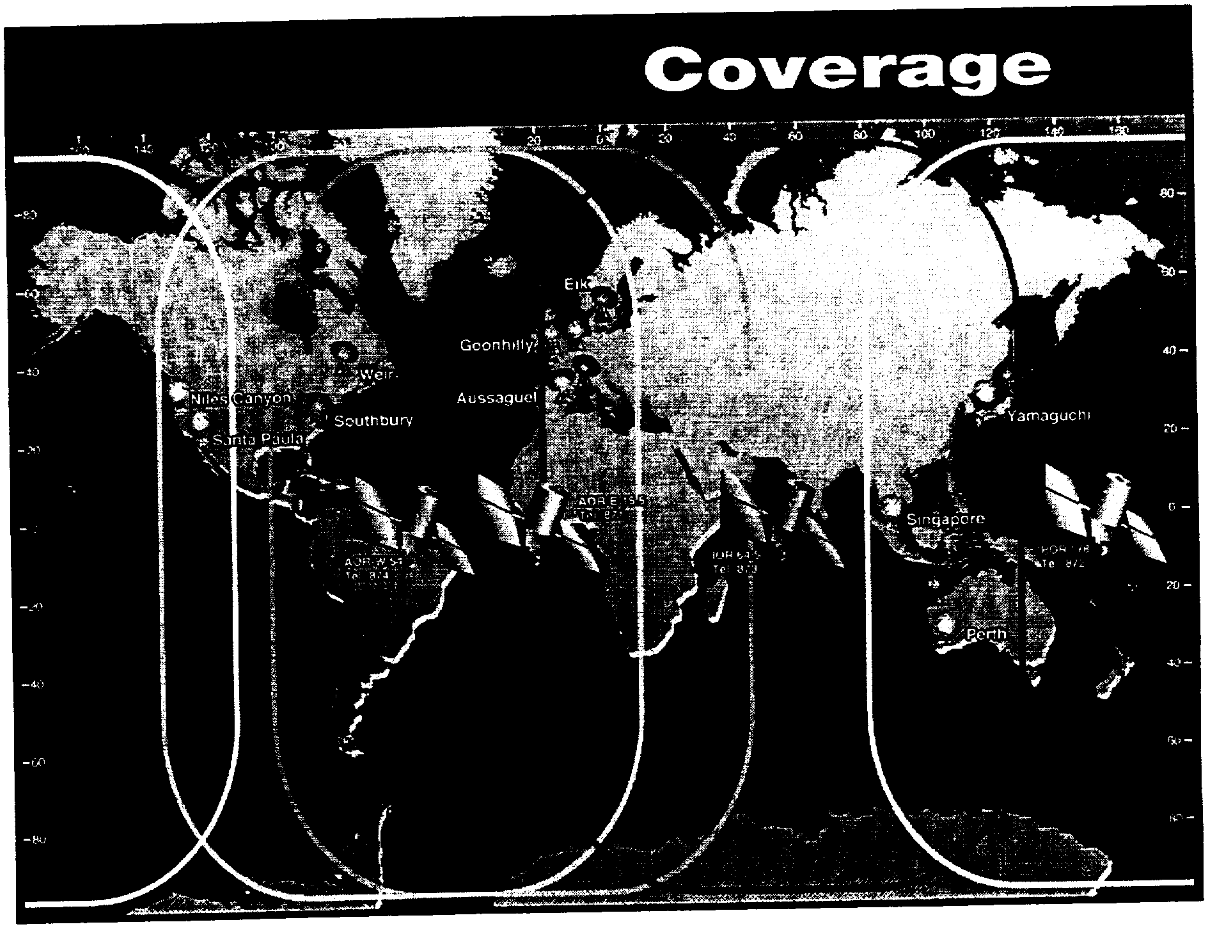
Figure 15. Master Station and Antenna Components



Unlike other WAAS subsystems, the WAAS-GPS receiver is not common to the entire TRACON, but instead each aircraft has an independent WAAS-GPS receiver. Because of this distinction, the WAAS-GPS receiver was not modeled within the context of the common WAAS subsystems, but instead treated as a separate system. For additional information regarding the WAAS-GPS receiver reliability analysis refer to the section on WAAS-GPS receiver.

Inmarsat-3 provides the geosynchronous communication satellite coverage. Inmarsat-3 satellites include a navigational payload for augmentation of GPS and Glonass, which is compatible with the FAA's WAAS and the European equivalent. Inmarsat-3 includes 4 operational satellites plus 1 on-orbit spare. Figure 16 shows the locations of the Inmarsat-3 satellites, named Atlantic Ocean Region – West (**AOR-W**), Atlantic Ocean Region – East (**AOR-E**), Indian Ocean Region (**IOR**), and Pacific Ocean Region (**POR**). The spare orbits at 25 degrees east (between **AOR-E** and **IOR**). Two satellites provide WAAS coverage (**POR** and **AOR-W**). A third satellite has coverage over continental United States (**AOR-E**), however, its navigation payload is reserved for the European system. Operational assumptions in the event of a satellite failure were based on engineering judgement. If **AOR-W** fails, it was assumed that **AOR-E** would be redirected to serve WAAS. If **AOR-W** or **POR** fails, it is assumed that remaining operational satellites would be repositioned to provide complete continental United States coverage.

Figure 16. Inmarsat 3 Geosynchronous Communications Satellite Coverage



Ground-Earth Stations are uplink antennas to Inmarsat communication satellites. The ground earth stations are normally trained on a specific communication satellite. Ground-earth stations along the North American east coast uplink to the **AOR-W** communication satellite, while ground-earth stations along the North American west coast uplink to the **POR** communication satellite. East coast antennas are located at **Southbury**, Laurentides (**Weir**), and Staten Island. West coast antennas are located at **Santa Paula** and **Niles Canyon**.

WAAS navigation functional states include Fully Operational, 3 Degraded Modes, Failed Safe and Failed Unsafe. The Fully Operational state is defined as augmented GPS signal accuracy with integrity notification. This state occurs when the system is operating normally. CAT-I approaches would be allowed. The Degraded Mode 1 state is defined as augmented GPS signal accuracy without integrity notification. This state occurs when the WAAS integrity monitoring signal is unavailable, but the system is otherwise operating normally. In this case, CAT-I approaches could be allowed, but with low confidence in position estimate. The Degraded Mode 2 state is defined as standard GPS signal accuracy with integrity notification. This state occurs when the WAAS position correction signal is unavailable, but the system is otherwise operating normally. In this case, non-precision approaches are allowed, but not CAT-I approaches. The Degraded Mode 3 state is defined as standard GPS signal accuracy without integrity notification. This state occurs when WAAS position correction and integrity monitoring signals are unavailable, but the system is otherwise operating normally. In this case, non-precision approaches could be allowed, but with low confidence in position estimate. The Failed Safe state is defined as no GPS position estimate. This state occurs when less than 4 satellite ranging signals are available. In this case, approach requires an alternate navigation system. The Failed Unsafe state is defined as a GPS position estimate that is unknowingly incorrect. This state occurs when there is an undetected system error. In this case, approaches are allowed but with a decision height violation. This state leads to potentially hazardous operations.

WAAS GPS Receiver

The WAAS GPS Receiver is onboard each equipped aircraft and provides the crew with the position estimate of the aircraft. It receives the signals from the GPS satellites in view and from the geosynchronous communication satellite covering its location. The signal from the GPS satellites provides the ranging information for position determination. The signal from communication satellite provides an additional signal for ranging, but also provides the position correction and integrity monitoring information. The WAAS GPS Receiver processes the signals from the satellites.

Different aircraft could be equipped with WAAS GPS Receivers differing in design and reliability. The current safety tool provides the design shown in Figure 17. Future versions of the tool could provide more comprehensive or different designs than what will be described here.

Figure 17. WAAS GPS Receiver

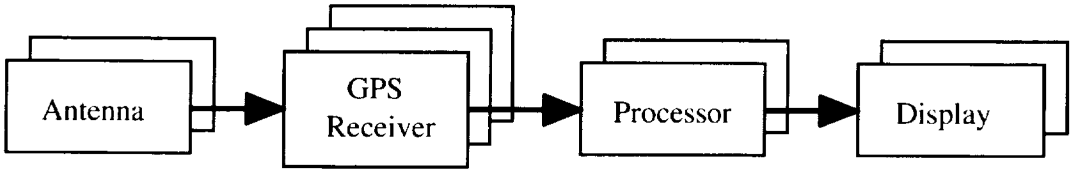


Figure 17 shows the WAAS GPS Receiver is made up of four types of components—Antennas, GPS Receivers, Processors, and Displays. The duplicate blocks indicate the redundancy of each type of component. That is, there are two redundant Antennas, three redundant GPS Receivers, two redundant Processors, and two redundant Displays. Arrows indicate the connections between the components. Connected components are fully cross-strapped. For example, the connection between the GPS Receivers and the Processors indicated by the arrow means each of the 3 GPS Receivers is connected to each of the Processors. All redundant components are assumed to be on-line if functional.

The WAAS GPS Receiver function is defined to have three states – Fully Operational, Failed Safe, and Failed Uncovered. The WAAS GPS Receiver is Fully Operational as long as 1 Antenna, 1 GPS Receiver, 1 Processor, and 1 Display are functional. The WAAS GPS Receiver function remains Fully Operational as failures occur as long as the Failure Detection, Isolation and Reconfiguration (FDIR) process successfully detects and removes component failures. The Failed Safe state results if the FDIR process successfully detects and removes a component failure, but the minimum number of components of each type are no longer functional. If this occurs, the WAAS GPS Receiver provides an alert to the crew. If a failure of a component should occur and the FDIR process does not detect or remove it, this results in the Failed Uncovered state.

The ASSIST program is used to construct the Markov model, which is used to predict the probability of being in each of the three function states. Appendix H presents the ASSIST input file used to generate the Markov model for the WAAS GPS Receiver. Note that the ASSIST input file is set up so that the number of redundant components, the failure rates and coverage probabilities for each component type can be changed.

When the aircraft takes off it is assumed to have no failures. The Markov model for the WAAS GPS Receiver will predict the probability of being in each of the functional states for the time period it is in the TRACON air space.

Impact

The Impact models map the failure configurations of the Reliability Model to the input parameters to the TRACON simulation.

Table 2 presents the Impact model for the WAAS GPS Receiver. When Fully Operational, the WAAS GPS Receiver provides sufficient navigational information to allow the aircraft to perform a Category I approach. If the WAAS GPS Receiver is failed and the aircraft crew is aware of its failure (Failed Safe state), another navigation system would be required to perform the approach. When the WAAS GPS Receiver is in the Failed Uncovered state, it means the WAAS GPS Receiver is failed, but the crew is unaware of its failure and is relying on incorrect navigation information.

Table 2. WAAS GPS Receiver Operational States

State of function	State definition	System impact	Simulation impact
Fully Operational	GPS Receiver fully operational, including integrity checking	If signals from GPS and Communication satellites are available, augmented GPS navigation accuracy with integrity is available	CAT I approach allowed with high confidence in position estimate
Failed Safe	WAAS GPS Receiver is unavailable and crew is alerted of loss	No position estimate from GPS	Approach requires alternative navigation system
Failed Uncovered	Undetected failure of WAAS GPS Receiver	Reliance on incorrect position estimate	CAT I approach allowed but undetected failure results in decision height violation

Table 3 presents the Impact model for the radar systems.

Table 3. Terminal Radar Approach Control Surveillance Operational States

State of function	State definition	System impact	Simulation impact
Fully Operational	Primary radar indication of all aircraft in TRACON; secondary radar data available for all aircraft equipped with functioning transponders	Position estimate of all aircraft in TRACON presented to controller is sufficient to control normal approach	Normal position errors and flight paths for all aircraft
Primary only	Loss of secondary radar	Position estimate of all aircraft in TRACON presented to controller is limited to accuracy provided by primary radar	Vertical position error of all aircraft with functioning transponders increased from normal to reflect loss of secondary radar information
Secondary only	Loss of primary radar	Position estimate available only for aircraft with functioning transponders	Position error of all aircraft without functioning transponder increased from normal to reflect loss of primary radar
Failed	Primary and secondary radar not functioning	Aircraft permitted to land but under contingency procedures	Position error of all aircraft increased from normal to reflect loss of primary and secondary radar information

Table 4 presents the Impact model for the ADS-B/Surveillance Data Link function. When Fully Operational, the ADS-B/Surveillance Data Link will allow the aircraft to perform an approach in which an operating ADS-B/Surveillance Data Link is required. If the ADS-B/Surveillance Data Link is failed and the crew is aware of the failure (Failed Safe state), this type of approach would not be allowed. If the aircraft is in the Failed Uncovered state, the ADS-B required approach is executed, but the other ADS-B equipped aircraft will be relying on incorrect position information (or none at all) and/or the crew will be relying on incorrect information from the ADS-B Displays.

Table 4. ADS-B/Surveillance Data Link Operational States

State of function	State definition	System impact	Simulation impact
Fully Operational	Valid broadcast and reception of broadcasts from other aircraft	Transmit and receive functions are fully available	ADS-B required approach allowed; aircraft able to detect other blundering aircraft equipped with ADS-B and other aircraft equipped with ADS-B can detect a blunder from this aircraft
Failed Safe	Invalid broadcast or unable to receive broadcasts from other aircraft and alert of capability loss	No longer able to perform ADS-B required approaches	Aircraft not allowed to perform ADS-B required approach
Failed Uncovered	Invalid broadcast or unable to receive broadcasts from other aircraft and no alert of capability loss	ADS-B required approach allowed but other aircraft do not receive valid surveillance data and/or aircraft is unaware of other aircraft in its vicinity	ADS-B required approach allowed but aircraft functions as if not equipped with ADS-B

Table 5 presents the approach systems Impact model.

Table 5. Airport Approach Operational States

State of function	State definition	System impact	Simulation impact
Fully Operational	Full functionality is available for precision approach of aircraft to runway	Approaches permitted under Instrument Flight Rules (IFR) for lowest allowable minimum ceiling and visibility requirements	Aircraft follow normal flight paths to runway
Degraded Loss of markers or lighting systems	Failure of a marker or light; descent path available with degraded support	Increased minimum ceiling and visibility requirements to conduct IFR approach and increased stress on pilot	Assuming low ceiling under IFR, aircraft precluded from approaching runway; desired flight paths changed to remaining available runways
Degraded Loss of descent path	Loss of descent path (glideslope)	Increased minimum ceiling and visibility requirements to conduct IFR approach and increased stress on pilot (increases are greater than those for other degraded state)	Assuming low ceiling under IFR, aircraft precluded from approaching runway; desired flight paths changed to remaining available runways
Failed	Loss of localizer; ground track not available for navigation to runway	Approaches to runway are no longer permitted under IFR	Assuming IFR, aircraft precluded from approaching runway; desired flight paths changed to remaining available runways

WAAS RELIABILITY MODELS

The WAAS system was modeled as four subsystems: GPS satellites, geosynchronous communication satellites, master station, and uplink antenna. The GPS and geosynchronous communication satellite models are based primarily on FAA specifications, whereas the master station and uplink antenna are based primarily on engineering judgement. Two WAAS subsystems, reference stations and ground network, were not modeled, since they are highly redundant and highly reliable.

SATELLITE FAILURE MODES

Geosynchronous communication and GPS satellite failure modes were defined by the FAA's WAAS specifications [7] as failure rates and mean durations. The geosynchronous communication satellites and GPS each have two failure modes. Each satellite system has a more frequent failure with shorter mean repair, and a less frequent failure with longer mean repair. The more frequent failures with shorter repair times represent software or system failures requiring re-initialization of satellite subsystems. The less frequent failures with longer repair times represent catastrophic failures requiring replacement of the satellite. GPS satellite repairs are defined to occur in series, while geosynchronous communication satellite repairs are defined to occur in parallel. Table 6 specifies each failure mode's failure rate and mean duration. The Markov models in this analysis assume only 1 failure per satellite at a time. The FAA specifications do not define modeling assumptions for the spare geosynchronous communication satellite; several modeling assumptions will be investigated.

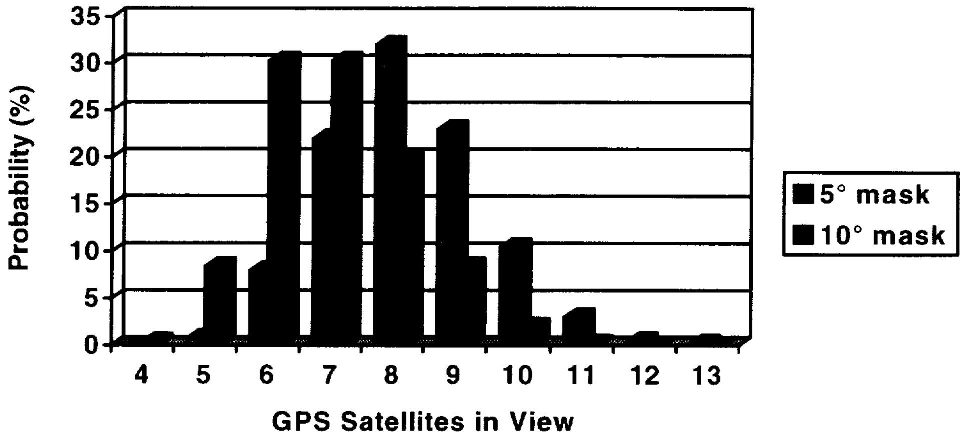
Table 6. GPS and Geosynchronous Communication Satellite Failure Modes

Failure Mode	Failure Rate	Mean Duration	Repairs in
GPS Mode 1	1.65 / yr	12.2 hr	Series
GPS Mode 2	0.16 / yr	1.25 mo	Series
GEO Comm Mode 1	0.083 / yr	19.8 hr	Parallel
GEO Comm Mode 2	0.014 / yr	3 yr	Parallel

GPS Modeling

Modeling of the GPS satellites is complicated by the fact that the number of satellites within view is time varying and depends on geometry. The number of GPS satellites in view for any geographic location varies slowly between 4 and 13. The analysis method allows the number of GPS satellites to be varied and averaged depending on the geographic location. For example, Figure 18 gives the probability of number of GPS satellites in view at 35-degree latitude with 5 degree and 10-degree elevation mask angles. The analysis runs the Markov model for 4 to 13 GPS satellites and averages the results based on these or similar probabilities.

Figure 18. Probability of Number of GPS Satellites in View



Geosynchronous Communication Satellite Modeling

Inmarsat's geosynchronous communication satellites provide constant worldwide satellite coverage. The western United States is covered by two communication satellites, central United States is covered by one communication satellite, and eastern United States by one communication satellite. A spare communication satellite is on-orbit, however its operational procedures are not well defined in the literature. Therefore three modeling options of spare usage are included: no spare, local spare, and global spare. The first modeling option assumes there is no spare available, illustrated in Figure 19. This simplified option follows the FAA specifications exactly. The second modeling option assumes there is a local spare available, illustrated in Figure 20. This option is accurate for all Inmarsat satellite functions, except WAAS. The local spare model assumes the spare can be operational within 1 month, the spare cannot fail until it becomes operational (i.e., cold spare), and the spare is activated only when the communication satellite has a long-term failure. The third modeling option assumes there is one global spare available, illustrated in Figure 21. This is the most complicated and realistic modeling option for the Inmarsat's WAAS capability. The global spare model assumes the spare can be operational within 1 month, the spare can fail before it becomes operational, and the spare is activated for both long and short-term communication satellite failures. The spare usage strategies are modeled only with 1 communication satellite, as this is the bounding case. In Figures 19 and 20, each node specifies the number of operational satellites, failures are given as rates, and repairs are given as mean durations.

Figure 19. Geosynchronous Communication Satellite Coverage Model With No Spare

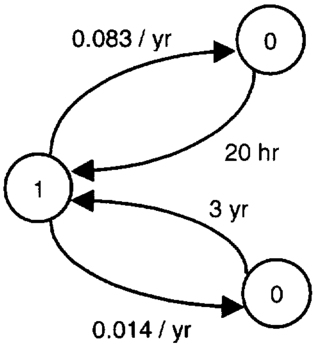


Figure 20. Geosynchronous Communication Satellite Coverage Model With Local Spare

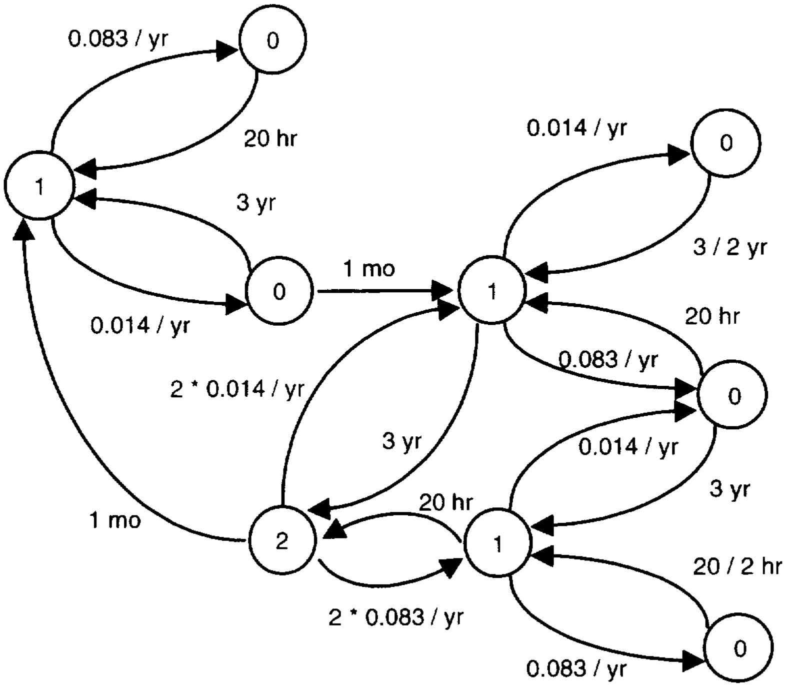
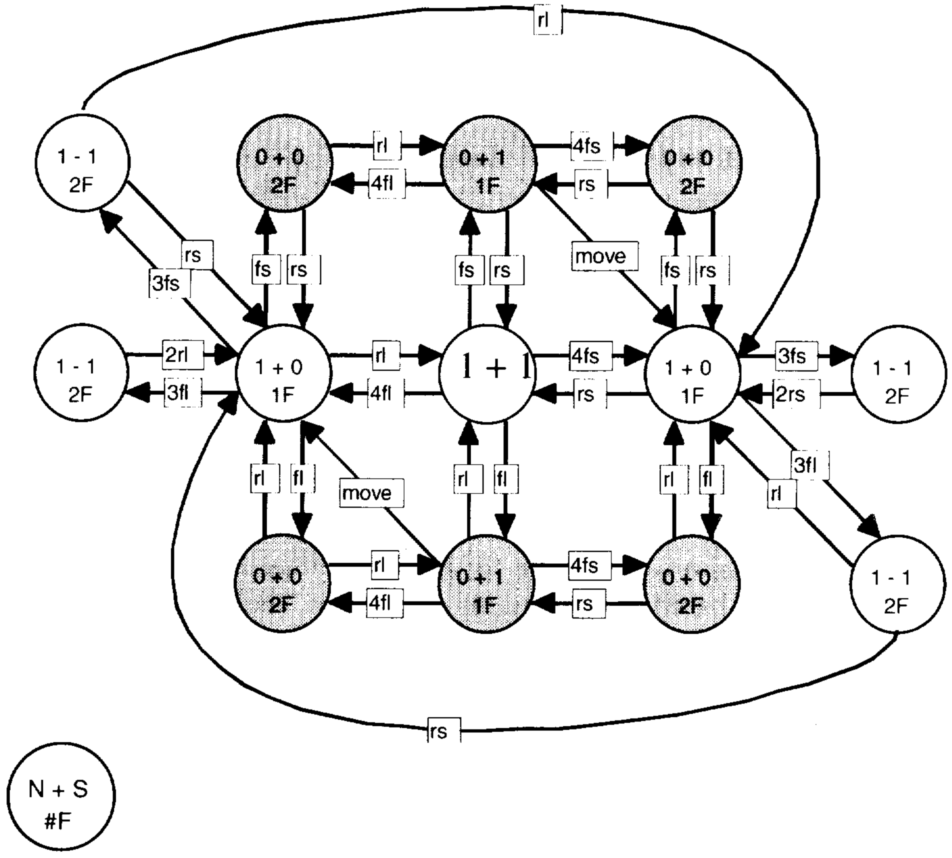


Figure 21. Geosynchronous Communication Satellite Coverage Model With Global Spare



The state transition diagram for the geosynchronous communication satellite with global spare is displayed in Figure 21. The state transition diagram assumes 5 operational satellites are in-orbit, 4 satellites provide global coverage and 1 satellite acts as a "hot" spare. ("Hot" implies the spare can fail while it is inactive.) Of the 4 global satellites, 1 provides coverage locally. In the figure, operational states are displayed in white; failed states are shaded in gray. In the key, *N* represents local communication satellite coverage, where 1 implies local coverage and 0 implies *no* local coverage. Also, *S* represents the availability of a spare communication satellite. The range of *S* is 1 to –3; 1 implies there is a spare available, 0 implies no spare is available, and a negative value implies there is a shortage of working satellites. Finally, *#F* is the total number of concurrent failures. Only two concurrent failures are modeled for the entire system. The failure transition rates are given by *fl* and *fs*. The repair transition rates are given by *rl* and *rs*. The less frequent failure with slower repair is given by *fl* and *rl*, while the more frequent failure with faster repair is given by *fs* and *rs*. A satellite can be in one mode or the other, but not both. The spare satellite can be repositioned with transition rate, *move*, to provide local coverage for both long and short failures of the local communication satellite. When the local satellite is repaired, it assumes the role of spare without an additional transition. If any other satellite in the system fails, then the spare is not available.

The ASSIST models for generating the Markov reliability models for the communication satellites are in Appendices I, J, and K.

MASTER STATION MODELING

The WAAS Master Station includes two major components, a master clock and a master computer. The master computer can be further subdivided into the hardware, software, and operating system. The software includes both position correction and integrity monitoring algorithms. Two models were created: one including both the master clock and computer, and another including just the master computer. Since the state size explodes for the model including both the clock and computer, the number of simultaneous failures is limited to 2 in the complete model. Even with this limitation, the model still has very slow execution. Since the master clock is assumed to be highly reliable, the model excluding the master clock is recommended. FAA specifications define failure, recovery, and coverage rates only for software failures, operating system recovery, and integrity monitoring software coverage. All other failure, recovery, and coverage rates were based on engineering judgement. The master station modeling assumes 2 master clocks and 3 master computers. Only the software may have undetected failures, all other components are assumed to have 100 percent coverage probabilities. The position correction coverage probability was assumed to be the same as the integrity monitoring coverage probability. Software errors are assumed to recover on the next software cycle. Master clock failures were assumed to be low probability, 1 in 10000 days; master computer hardware failures were assumed to be mid probability, 1 in 1000 days; and master computer operating system failures were assumed to high probability, 1 in 100 days. Recovery rates for the master clock and computer hardware were assumed to be 12 and 6 hrs, respectively. The recovery rate for the operating system is specified as 10 min Appendices L and M give the ASSIST models for the Master Station.

GROUND-EARTH STATION MODELING

The Ground-Earth Station modeling consists of two uplink antennas and the signal transmission. The FAA specifications define only the transmission failure rate. A transmission failure was assumed to recover on the next software cycle. The antenna failure and recover rates were based on engineering judgement Appendix N gives the ASSIST model for transmission.

WAAS IMPACT MODEL

The Impact model for WAAS is presented in Table 7. The states of this model include the ability of GPS receivers to (redundantly and independently) monitor signal integrity if 5 or more ranging signals are available.

Table 7. WAAS Navigation Functional States

WAAS Navigation	State Definition	State Impact	Simulation Impact
Fully Operational Augmented w/ Integrity	GEO position correction and integrity monitoring signals available; 4 or more GEO and GPS ranging signals available Or GEO position correction signal available, but integrity monitoring signal unavailable; 5 or more GEO and GPS ranging signals available and GPS receiver includes integrity checking	Augmented GPS accuracy w/ integrity (7.6 m 95 percent horizontal and vertical accuracy w/ 5.2 sec integrity notification)	CAT I approach allowed w/ high confidence in position estimate
Degraded Mode 1 Augmented w/o Integrity	GEO position correction signal available, but integrity monitoring signal unavailable, 4 GEO and GPS ranging signals available or GPS receiver does not include integrity checking	Augmented GPS accuracy w/o integrity (7.6 m 95 percent horizontal and vertical accuracy w/ 15 min integrity notification)	CAT I approach allowed w/ low confidence in position estimate
Degraded Mode 2 Standard w/ Integrity	GEO position correction signal unavailable, but integrity monitoring signal available; 4 or more GEO and GPS ranging signals available Or GEO position correction and integrity monitoring signals unavailable; 5 or more GEO and GPS ranging signals available and GPS receiver includes integrity checking	Standard GPS accuracy w/ integrity (100 m 95 percent horizontal accuracy w/ fast integrity notification)	Non-precision approach allowed w/ high confidence in position estimate

Table 7. WAAS Navigation Functional States

WAAS Navigation	State Definition	State Impact	Simulation Impact
Degraded Mode 3 Standard w/o Integrity	GEO position correction and integrity monitoring signals unavailable; 4 GEO and GPS ranging signals available or GPS receiver does not include integrity checking	Standard GPS accuracy w/o integrity (100 m 95 percent horizontal accuracy w/ 15 min integrity notification)	Non-precision approach allowed w/ low confidence in position estimate
Failed Safe Unknown	Less than 4 GEO and GPS ranging signals available	No position estimate	Approach requires alternate navigation system
Failed Unsafe Incorrect	Undetected system error	Incorrect position estimate	CAT I or non-precision approach allowed w/ decision height violation

Table 8 details the mapping logic based on the state definitions for the WAAS navigational modes. The mapping logic assumes the aircraft's GPS receiver includes operational integrity monitoring software. GEO is the number of geosynchronous communication satellites in range with operational ranging signal and GPS is the number of GPS satellites in range with operational ranging signal. PC is the position correction signal availability and IM is the integrity monitoring signal availability. PC and IM may be TRUE, FALSE, or ERROR. TRUE implies the master clock, master computer, master algorithm, uplink antenna, signal transmission, and communication satellite are *all* operational. FALSE implies master clock, master computer, master algorithm, uplink antenna, signal transmission, and communication satellite are *not all* operational. ERROR implies the master algorithm returns a solution, but that the solution is incorrect.

Table 8. WAAS Navigation Functional State Mapping

WAAS Navigation	State Definition	Mapping Logic
Fully Operational Augmented w/ Integrity	Comsat position correction and integrity monitoring signals available; 4 or more Comsat and GPS ranging signals available Or Comsat position correction signal available, but integrity monitoring signal unavailable; 5 or more Comsat and GPS ranging signals available	(PC = TRUE && IM = TRUE && GEO + GPS > 3) || (PC = TRUE && IM = FALSE && GEO + GPS >4)

Table 9. WAAS Navigation Functional State Mapping (Continued)

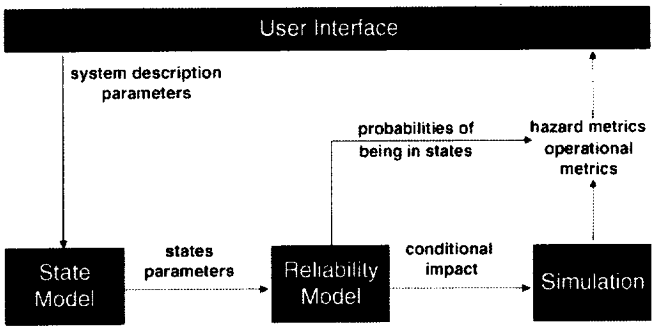
WAAS Navigation	State Definition	Mapping Logic
Degraded Mode 1 Augmented w/o Integrity	Comsat position correction signal available, but integrity monitoring signal unavailable, 4 Comsat and GPS ranging signals available	(PC = TRUE && IM = FALSE && GEO + GPS = 4)
Degraded Mode 2 Standard w/ Integrity	Comsat position correction signal unavailable, but integrity monitoring signal available; 4 or more Comsat and GPS ranging signals available Or Comsat position correction and integrity monitoring signals unavailable; 5 or more Comsat and GPS ranging signals available	(PC = FALSE && IM = FALSE && GEO + GPS > 4) || (PC = FALSE && IM = TRUE && GEO + GPS >3)
Degraded Mode 3 Standard w/o Integrity	Comsat position correction and integrity monitoring signals unavailable; 4 Comsat and GPS ranging signals available	(PC = FALSE && IM = FALSE && GEO + GPS = 4)
Failed Safe	Less than 4 Comsat and GPS ranging signals available	GEO + GPS < 4
Unknown		

Failed Unsafe
Incorrect
	Undetected system error	PC = ERROR
		||
		IM = ERROR

ANALYSIS FRAMEWORK OVERVIEW

The top level conceptual framework for the analysis we have performed in this and previous projects consists of three types of analytic tools that interact with one another and are driven by a flexible user interface. This framework is illustrated in Figure 22. The specific tools used in any given application of this framework depend upon the analytical objective of the user.

Figure 22. Top Level View Analysis Framework


User Interface
system description parameters
probabilities of being in states
hazard metrics operational metrics
states parameters
conditional impact
State Model
Reliability Model
Simulation

In general, in the first major element of the framework, the user specifies the problem he or she wishes to solve by creating state models of the objects involved in the problem. In the present instance, for example, the user creates the user creates Markovian state models of the key elements of a TRACON, aircraft, and WAAS. The parameters characterizing the states would include those required to define the various possible levels of operational performance (e.g., from fully operational, through various levels of degradation, to inoperative) as well as state transition rates (for continuous time models) or probabilities (for discrete time models).

The second major element of the framework consists of more or less traditional reliability modeling of the various objects. These models would typically model specific hardware and software systems. The output of these models is used in two ways. First, the operational impact of being in a given state defines the behavior of the associated object in a dynamic operational scenario. And second, the probability of being in that given state is used to weigh the results of the scenario.

The third major element of the framework is a simulation with sufficient fidelity to model the operational scenarios of interest. To date implementation of this element of the framework has evolved from a simulation of several aircraft landing on closely spaced parallel runways, through a simplified dynamic model of a TRACON handling a hundred or more inbound, landing aircraft, to a more detailed event-sequenced, object oriented simulation of a TRACON.

It is envisioned that the models in this framework will typically be exercised to evaluate some proposed new hardware, software, or procedural element of the civil air traffic system prior to its introduction into use. The user would define the problem using the state model tools, run the reliability models, define the operational impact of the various states of interest, run the simulation a number of times to generate comparative baselines and state-dependent predictions of future operations, and then weigh the results by the appropriate state probabilities. The results would consist of safety and economic measures. Safety measures would typically consist of frequencies of occurrence of various hazardous situations. Economic measures would consist of costs (investment and operating) and throughput (number of aircraft handled per unit time).

EXAMPLE SYSTEM RESULTS

This section illustrates the application of the reliability portion, TARAT (Terminal Area Reliability Analysis Tool), of the Integrated System Analysis Tool described previously. As evidenced in Appendix O, the user can interact with TARAT at two levels. At the top level, a user can specify the system at the level of high-level system design, e.g., WAAS without ILS, WAAS with ILS. In addition, the user can specify details about the top-level system components, e.g., the spare policy of the communication satellite. This is done in the TARAT input file, (Appendix O). At the lower level, the user can change individual component parameters, e.g., mean time to failure, mean time to repair. This is done in the ASSIST input files.

As an illustration, the following is an analysis of WAAS versus ILS as the technology used for Category I landings, i.e., the system has WAAS or ILS, but not both. It should be emphasized that the numerical results should be taken as notional, since we were unable to validate them at this time.

Table 9 lists results for WAAS system state reliabilities for a location at 35-degree latitude with a 5-degree mask angle, geo-synchronous communication satellite with one global spare, master station with master computer only, and nominal uplink antenna. The WAAS system was modeled as four independent subsystems: GPS satellites, geo-synchronous communication satellites, master station, and uplink antenna. The results have been normalized to account for numerical approximations of the *PAWS* routine.

Table 9. WAAS Navigation Functional Reliability Results

WAAS Navigation	Reliability
Fully operational Augmented GPS w/integrity	0.99478
Degraded model Augmented GPS w/o integrity	6 x 10^{-9}
Degraded model 2 Standard GPS w/integrity	0.00521
Degraded model 3 Standard GPS w/o integrity	8 x 10^{-6}
Failed safe Unknown	6 x 10^{-6}
Failed unsafe Incorrect	8 x 10^{-8}

Table 10 shows a summary of the reliabilities of the individual options. State reliabilities within the table are listed as N/A if the states are not defined within those models, e.g., there is no Degraded Modes 1, 2 or 3 for the Receiver model. The reliability values are the probabilities shown in Table 9 that are combined with the metrics generated by the simulation program.

The WAAS subsystem can be defined with a variety of options. There are 3 sparing options available of either no spares available, local sparing available, or global sparing available using either the computer or clock computer.

The ILS system has the option of defining the repair option being either to repair in a nominal mode or an option to delay the repairs a specified amount of time.

Table 10. Summary of system reliability

				WAAS computer			WAAS clock computer			
	Radar	Receiver	No spare	Global Spare	Local Spare	No spare	Global Spare	Local Spare	ILS(nom)	ILS(delay)
Fully Operational	0.990445	0.999998	0.959360	0.994772	0.997783	0.959361	0.994814	0.997783	0.989729	0.816773
Degraded Mode 1	0.002907	N/A	5.76E-09	5.98E-09	5.99E-09	5.76E-09	5.98E-09	5.99E-09	0.007942	0.174961
Degraded Mode 2	0.003976	N/A	0.040564	0.005214	0.002207	0.040563	0.005172	0.002207	0.000998	0.006935
Degraded Mode 3	N/A	N/A	6.61E-05	8.42E-06	3.51E-06	6.61E-05	8.42E-06	3.51E-06	N/A	N/A
Failed Safe	0.002673	3.15E-08	1.01E-05	6.21E-06	5.88E-06	1.01E-05	6.21E-06	5.88E-06	0.001332	0.001332
Failed Unsafe	N/A	1.922E-06	7.68E-08	7.97E-08	7.99E-08	7.68E-08	7.9E-08	7.99E-08	N/A	N/A
Total Probability	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

We compare WAAS and Receiver against the ILS system. Combining the probability of the WAAS and the Receiver models for a Category I approach generates the following table. Listed below are the probabilities given one of the different scenarios that can occur within WAAS.

Table 11 lists the system reliability (i.e., the probability the system is operational for Category I landings) for several options of the WAAS and Receiver models.

Table 11. Combining WAAS and Receiver for Category I Approaches.

WAAS * RECEIVER			WAAS * RECEIVER		
	computer			clock computer	
No spare	Global Spare	Local Spare	No spare	Global Spare	Local Spare
0.959358	0.9947697	0.997781	0.959359	0.994812	0.997781

As an example of the type of conclusion a user might make, it appears that there is minimal gain from selecting the system to use the clock computer over the regular computer.

From Table 10, the reliability of the ILS is 0.9897291. Comparing the results in Table 11 against this value, the option of WAAS and receiver is less reliable when there is no communication satellite spare and more reliable when there is a spare. Note that these conclusions are drawn before the simulation is run and should be understood in that context.

References

[1] S. C. Johnson, ASSIST User's Manual NASA Technical Memorandum 87735, August 1986.

[2] R. W. Butler and P. H. Stevenson, The PAWS and STEM Reliability Analysis Programs, NASA Technical Memorandum 100572, March 1988.

[3] D. P. Hanson, Tarat READMEî http://www.dc.draper.com/~dphanson/README.tarat, 17 November 1998.

[4] D. P. Hanson and P. Scheidler, Jr., WAAS Reliability Analysis, Draper Presentation, July 1998.

[5] Parkinson and Spilker, Editors, Axlerad and Enge, Associate Editors, Global Positioning System: Theory and Applications, Volume I, Chapter 5, AIAA, 1996.

[6] Parkinson and Spilker, Editors, Axlerad and Enge, Associate Editors, Global Positioning System: Theory and Applications, Volume II, Chapter 12, AIAA, 1996.

[7] U.S. Department of Transportation, Federal Aviation Administration Specification, Wide Area Augmentation System (WAAS), FAA-E-2892B, 10 March 1997.

[8] Federal Aviation Association, ATCA Briefing, FAA 369 ATCA, 16 April 1998.

[9] G. Trevitt, Inmarsat's Family of Satellites, January 1998.

[10] G. Kinal, Inmarsat Services For Navigation, February 1998.

[11] D. Featherstone, Communications, Navigation and Surveillance Inmarsat's Role in Aeronautical Satcoms.

[12] R. Fuller, R. Johnston, and N. McDonald, *Human Factors in Aviation Operations*, University Press, Cambridge, Great Britain, 1995.

[13] D. V. Hopkin, *Human Factors in Air Traffic Control*, Taylor and Francis, Bristol, PA, 1995.

[14] R. E. Hurst, *Pilot Error*, Granada Publishing, New York, NY, 1982.

[15] ICAO Circular, Human Factors Digest No. 8: Human Factors in Air Traffic Control, ICAO, Montreal, Canada, 1993.

[16] N. G. Leveson, Safeware: System Safety and Computers a Guide to Preventing Accidents and Losses Caused by Technology, Addison-Wesley, Reading, MA, 1995.

[17] N. G. Leveson, Safety Analysis of Air Traffic Control Upgrades, Final Report, 1997.

[18] C. D. Wickens, *Flight to the Future: Human Factors in Air Traffic Control*, National Academy Press, Washington, D.C., 1997.

[19] P. F. Kostiuk, M. B. Adams, D. F. Allinger, G. Rosch and J. K. Kuchar, An Integrated Safety Analysis Methodology for Emerging Air Transport Technologies , NASA/CR-1998-207661, April 1998, pp. 64.

[20] P. F. Kostiuk, G. Shapiro, D. Hanson, S. Kolitz, F. Leong, G. Rosch and C. Bonesteel, A Method for Evaluating the Safety Impacts of Air Traffic Automation , NASA/CR-1998-207673, May 1998, pp. 74.

Appendix A
Simulation Model

The simulation model for the Integrated Safety Analysis Tool is under continuing development. By the end of 1999, ISAT will be available for use by researchers in the aviation community through the Aviation Systems Analysis Capability (ASAC) web site, http://www.asac.lmi.org . For more information about becoming an ASAC user, please visit that web site.

In this Appendix, the capabilities of the ISAT simulation model are described, as they are planned when the model is available through ASAC. Documentation will be available on ASAC to provide up to date information, as well as input file formats.

The ISAT simulation model is written in MODSIM III, an object-oriented

simulation language.

The simulation model input data describes: the physical features of the TRACON and its constituent airports; the performance parameters for the physical infrastructure, aircraft, pilots and controllers, by performance state; and specification of the weather conditions, traffic, number of controllers, flight paths within the TRACON, and failure to be investigated.

Once initialized, the simulation will generate and move arriving aircraft for a time period sufficient to allow typical congestion to build up. After this initialization period, the failure to be investigated is injected into the simulation, by changing the appropriate state variable, and the performance of the system with the modified performance parameters describing this failure state are collected. With each failure is associated an amount of simulated time to continue running the simulation and collecting data after the failure.

The performance data collected includes the number of violations of the separation requirements, together with the associated closest approach and time to closest approach for each violation. The latter figures are an indication of the severity of the separation violation.

Aircraft movement in the simulation is governed by aircraft performance characteristics, which depend upon the state of the aircraft's control systems. In the current model, failures of aircraft control systems are not modeled; hence these values remain the same for a given aircraft throughout the simulation. The input data allows the user to define a number of different aircraft types (for purposes of determining separation requirements), and within each type, any number of performance classes, each of which can have different characteristics. The user also specifies the percentage of each aircraft type in the TRACON's traffic, and the percentage of each performance class within the type.

Aircraft are generated by the model to appear at the corner posts of the TRACON, with a nominal speed, heading, and altitude. The actual position, speed, and heading at which an aircraft appears are determined by its navigational state. The navigational state parameters are standard deviations from nominal. The actual deviation of each aircraft is randomly generated.

The simulated controller for the corner post receives a hand-off request message for each arriving aircraft. The controller has one or more, (depending upon the number of active runways in the weather determined configuration), potential flight paths to which the new arrival can be assigned. The flight paths are ordered by desirability. The controller associates the arrival with the first flight path from that corner post for which there is no anticipated conflict. If there is not a flight path that the controller determines is suitable, then the handoff is refused, and the aircraft is removed from the simulation.

A controller's ability to predict conflicts is determined by the controller's performance state and by the TRACON's surveillance state; however, in the current model, the controllers are assumed to operate at peak performance levels at all times. The TRACON's surveillance state determines the difference between the aircraft's actual position, and its position as perceived by a controller. For those surveillance states that correspond to functioning secondary radar, the aircraft's transponder state will also play a role in the reported position.

Once the aircraft has been assigned a flight path, the controller waits to be contacted by the arriving aircraft. The aircraft is then given directions for speed, heading and altitude that will bring it to the next point on the flight path. To model the ability to "trombone" arriving traffic, some flight path points are designated as having a range of acceptable values that the controller can assign to each aircraft. The model has been designed to allow the aircraft to know the next point and the time to reach it, or to know an entire 4-dimensional flight path. In the current version, the aircraft has no knowledge of the next desired point; the controller maintains this information.

The aircraft's response to the controller's direction is modeled by changing the aircraft's altitude, speed and heading, according to its performance characteristics. Based on these characteristics, the speed, heading, and position five seconds into the future are determined, and an event is scheduled to place the aircraft at that new location.

Communications between the aircraft and the controller may be damaged (stepped on), if two aircraft desire to send messages within a very short time of each other. The controller can detect this occurrence, and will be scheduled to ask aircraft to repeat the message. The pilot's human factor state may also result in a failure of the pilot to react to an instruction; however, in the current model, the pilots are assumed to operate at peak performance levels at all times.

The controller performs a scan of each aircraft, and monitors its progress towards the intended point. Instructions are issued when the aircraft is close to reaching a flight path point, when the aircraft's progress towards that point is less than satisfactory, or to resolve a conflict.

Appendix B
Primary Radar Model

```
 (* ASSIST model generates the states for the Primary Radar com-
ponents *)
LIST = 3;
PRUNE = 0;
STATES = 1;

F_PRIM_RAD_ANT = 1/1000;    (* Primary radar Antenna *)
R_PRIM_RAD_ANT = 1/4;       (* MTTR - Primary radar Antenna *)
F_PRIM_RAD_TRN = 1/750;     (* Primary radar Transmitter Channel A
*)
R_PRIM_RAD_TRN = 1/2;       (* MTTR - Primary radar Transmitter
Channel A *)
F_PRIM_RAD_RCV = 1/750;     (* Primary radar reciever Channel A *)
R_PRIM_RAD_RCV = 1/2;       (* MTTR - Primary radar reciever Chan-
nel A *)

SPACE = (SYS_MODE: 0..1, PRIM_RAD_ANT: 0..1, PRIM_RAD_TRN: 0..2,
PRIM_RAD_RCV: 0..2);

START = (1, 1, 2, 2);

(* Loss of Primary radar antenna is considered loss of the pri-
mary radar *)
IF PRIM_RAD_ANT > 0 TRANTO SYS_MODE = 0, PRIM_RAD_ANT =
PRIM_RAD_ANT - 1 BY F_PRIM_RAD_ANT;
IF PRIM_RAD_ANT < 1 TRANTO SYS_MODE = 1, PRIM_RAD_ANT =
PRIM_RAD_ANT + 1 BY R_PRIM_RAD_ANT;

(* Loss of both of the Primary radar transmitters is considered
loss of the primary radar *)
IF PRIM_RAD_TRN > 0 THEN
   IF PRIM_RAD_TRN = 1 THEN
      TRANTO SYS_MODE = 0, PRIM_RAD_TRN = PRIM_RAD_TRN - 1 BY
F_PRIM_RAD_TRN;
   ELSE
   TRANTO PRIM_RAD_TRN = PRIM_RAD_TRN - 1 BY F_PRIM_RAD_TRN;
   ENDIF;
ENDIF;

(* Repair strategy for the Primary transmitters checks to see if
repairing from loss of primary *)
IF PRIM_RAD_TRN < 2 THEN
   IF PRIM_RAD_TRN = 0 THEN
      TRANTO SYS_MODE = 1, PRIM_RAD_TRN = PRIM_RAD_TRN + 1 BY
R_PRIM_RAD_TRN;
   ELSE
   TRANTO PRIM_RAD_TRN = PRIM_RAD_TRN + 1 BY R_PRIM_RAD_TRN;
   ENDIF;
ENDIF;
```

```
(* Loss of both of the Primary radar receivers is considered loss
of the primary radar *)
IF PRIM_RAD_RCV > 0 THEN
   IF PRIM_RAD_RCV = 1 THEN
      TRANTO SYS_MODE = 0, PRIM_RAD_RCV = PRIM_RAD_RCV - 1 BY
F_PRIM_RAD_RCV;
   ELSE
   TRANTO PRIM_RAD_RCV = PRIM_RAD_RCV - 1 BY F_PRIM_RAD_RCV;
   ENDIF;
ENDIF;

(* Repair strategy for the Primary recievers checks to see if re-
pairing from loss of primary *)
IF PRIM_RAD_RCV < 2 THEN
   IF PRIM_RAD_RCV = 0 THEN
      TRANTO SYS_MODE = 1, PRIM_RAD_RCV = PRIM_RAD_RCV + 1 BY
R_PRIM_RAD_RCV;
   ELSE
   TRANTO PRIM_RAD_RCV = PRIM_RAD_RCV + 1 BY R_PRIM_RAD_RCV;
   ENDIF;
ENDIF;
```

Appendix C
Secondary Radar Model

```
(* ASSIST model generates the states for the Secondary Radar com-
ponents *)
LIST = 3;
PRUNE = 0;
STATES = 1;

F_SEC_RAD_ANT = 1/2500;    (* Secondary radar Antenna *)
R_SEC_RAD_ANT = 1/4;    (* MTTR - Secondary radar Antenna *)
F_SEC_RAD_INT = 1/1000;    (* Secondary radar interrogater Chan-
nel A/B *)
R_SEC_RAD_INT = 1/2;    (* MTTR - Secondary radar interrogater
Channel A/B *)
F_SEC_RAD_RCV = 1/2000;    (* Secondary radar receiver Channel
A/B *)
R_SEC_RAD_RCV = 1/2;    (* MTTR - Secondary radar receiver Chan-
nel A/B *)
F_SYNCH        = 1/1500;      (* Secondary synchronizer *)
R_SYNCH       = 1/2;    (* MTTR - Secondary synchronizer *)

SPACE = (SYS_MODE: 0..1, SEC_RAD_ANT: 0..1, SEC_RAD_INT: 0..2,
SEC_RAD_RCV: 0..2, SEC_SYNCH: 0..1);

START = (1, 1, 2, 2, 1);

(* Loss of Secondary radar antenna is considered loss of the sec-
ondary radar *)
IF SEC_RAD_ANT > 0 TRANTO SYS_MODE = 0, SEC_RAD_ANT = SEC_RAD_ANT
- 1 BY F_SEC_RAD_ANT;
IF SEC_RAD_ANT < 1 TRANTO SYS_MODE = 1, SEC_RAD_ANT = SEC_RAD_ANT
+ 1 BY R_SEC_RAD_ANT;

(* Loss of Synchronizer is considered loss of the secondary radar
*)
IF SEC_SYNCH > 0 TRANTO SYS_MODE = 0, SEC_SYNCH = SEC_SYNCH - 1
BY F_SYNCH;
IF SEC_SYNCH < 1 TRANTO SYS_MODE = 1, SEC_SYNCH = SEC_SYNCH + 1
BY R_SYNCH;

(* Loss of both of the Secondary radar interrogators is consid-
ered loss of the secondary radar *)
IF SEC_RAD_INT > 0 THEN
   IF SEC_RAD_INT = 1 THEN
      TRANTO SYS_MODE = 0, SEC_RAD_INT = SEC_RAD_INT - 1 BY
F_SEC_RAD_INT;
   ELSE
   TRANTO SEC_RAD_INT = SEC_RAD_INT - 1 BY F_SEC_RAD_INT;
   ENDIF;
ENDIF;
```

```
(* Repair strategy for the Secondary interrogators checks to see
if repairing from loss of secondary *)
IF SEC_RAD_INT < 2 THEN
  IF SEC_RAD_INT = 0 THEN
    TRANTO SYS_MODE = 1, SEC_RAD_INT = SEC_RAD_INT + 1 BY
R_SEC_RAD_INT;
  ELSE
  TRANTO SEC_RAD_INT = SEC_RAD_INT + 1 BY R_SEC_RAD_INT;
  ENDIF;
ENDIF;


(* Loss of both of the Secondary radar receivers is considered
loss of the secondary radar *)
IF SEC_RAD_RCV > 0 THEN
  IF SEC_RAD_RCV = 1 THEN
    TRANTO SYS_MODE = 0, SEC_RAD_RCV = SEC_RAD_RCV - 1 BY
F_SEC_RAD_RCV;
  ELSE
  TRANTO SEC_RAD_RCV = SEC_RAD_RCV - 1 BY F_SEC_RAD_RCV;
  ENDIF;
ENDIF;

(* Repair strategy for the Secondary receivers checks to see if
repairing from loss of secondary *)
IF SEC_RAD_RCV < 2 THEN
  IF SEC_RAD_RCV = 0 THEN
    TRANTO SYS_MODE = 1, SEC_RAD_RCV = SEC_RAD_RCV + 1 BY
R_SEC_RAD_RCV;
  ELSE
  TRANTO SEC_RAD_RCV = SEC_RAD_RCV + 1 BY R_SEC_RAD_RCV;
  ENDIF;
ENDIF;
```

Appendix D
Common Components Radar Model

```
(*models the radar components are common between primary/secondary*)

LIST = 3;
PRUNE = 0;
STATES = 1;
F_ANT_MT  = 1/1500;  (* Common Antenna Mount *)
R_ANT_MT  = 1/4;  (* MTTR - Common Antenna Mount *)
F_PRIM_PW = 1/3000;  (* Primary Power Source *)
R_PRIM_PW = 1/2;  (* MTTR - Primary Power Source *)
F_BACK_PW = 1/2000;  (* Backup Power Source *)
R_BACK_PW = 1/4;  (* MTTR - Backup Power Source *)
SPACE = (SYS_MODE: 0..1, ANT: 0..1, PRIM: 0..1, BACK: 0..1);
START = (1, 1, 1, 1);

IF ANT > 0 TRANTO SYS_MODE = 0, ANT = ANT - 1 BY F_ANT_MT;
IF ANT < 1 TRANTO SYS_MODE = 1, ANT = ANT + 1 BY R_ANT_MT;

(* If loss of both Primary and secondary power, considered loss of
radar *)
IF PRIM > 0 THEN
   IF BACK = 0 THEN
      TRANTO SYS_MODE = 0, PRIM = PRIM-1 BY F_PRIM_PW;
   ELSE
   TRANTO PRIM = PRIM - 1 BY F_PRIM_PW;
   ENDIF;
ENDIF;

(* repair strategy for primary power *)
IF PRIM < 1 THEN
   IF BACK = 0 THEN
      TRANTO SYS_MODE = 1, PRIM = PRIM + 1 BY R_PRIM_PW;
   ELSE
   TRANTO PRIM = PRIM + 1 BY R_PRIM_PW;
   ENDIF;
ENDIF;

(* If loss of both Primary and secondary power, considered loss of
radar *)
IF BACK > 0 THEN
   IF PRIM = 0 THEN
      TRANTO SYS_MODE = 0, BACK = BACK-1 BY F_BACK_PW;
   ELSE
   TRANTO BACK = BACK - 1 BY F_BACK_PW;
   ENDIF;
ENDIF;

(* repair strategy for backup power *)
IF BACK < 1 THEN
```

```
   IF PRIM = 0 THEN
      TRANTO SYS_MODE = 1, BACK = BACK + 1 BY R_BACK_PW;
   ELSE
   TRANTO BACK = BACK + 1 BY R_BACK_PW;
   ENDIF;
ENDIF;
```

Appendix E
ADS-B Model

```
(*  ASSIST Input File to Generate  *)
(*  ADS-B SURE Input File          *)


(*  Number of Redundant Components of Each Type  *)

n_ins =  2;    (* INS *)
n_proc = 2;    (* ADS-B Processors *)
n_dis =  2;    (* ADS-B Displays *)
n_tx =   1;    (* Modulator and Transmitter, n_tx <= 1*)
n_rx =   1;    (* Receiver and Demodulator, n_rx <= 1 *)
n_ant =  1;    (* Antenna, n_ant <= 1 *)


(*  Failure Rates  *)

l_ins =  1.0e-4;    (* INS *)
l_proc = 1.0e-5;    (* ADS-B Processors *)
l_dis =  2.0e-5;    (* ADS-B Displays *)
l_tx =   5.0e-5;    (* Modulator and Transmitter *)
l_rx =   5.0e-5;    (* Receiver and Demodulator *)
l_ant =  1.0e-6;    (* Antenna *)


(*  Coverage Probabilities  *)

c_ins_2 =  0.999;  (* INS, two on-line *)
c_ins_1 =  0.99;   (* INS, one on-line *)
c_proc_2 = 0.99;   (* ADS-B Processors, two on-line *)
c_proc_1 = 0.95;   (* ADS-B Processors, one on-line *)
c_dis_2 =  0.999;  (* ADS-B Displays, two on-line *)
c_dis_1 =  0.99;   (* ADS-B Displays, one on-line *)
c_tx =     0.99;   (* Modulator and Transmitter *)
c_rx =     0.99;   (* Receiver and Demodulator *)
c_ant =    1.00;   (* Antenna *)


(*  Other Parameters  *)

LIST = 3;                  (* Needed for the .mod file *)
n_modes = 2;               (* Number of system failure modes
which
                              will be differentiated in model *)


space = (m_ins: 0..n_ins,     (* Number of on-line INSs *)
         m_proc: 0..n_proc,   (* Number of on-line ASD-B Proces-
sors *)
```

```
         m_dis: 0..n_dis,      (* Number of on-line ASD-B Displays
*)
         m_tx: 0..n_tx,        (* Number of on-line Modulator and
Transmitter  channels *)
    m_rx: 0..n_rx,        (* Number of on-line Receiver and De-
modulator channels *)
    m_ant: 0..n_ant,      (* Number of on-line Antennae *)
         f_mode: 0..n_modes); (* Flag indicating system failure
mode
                                  0 = operational state,
                                  1 = failed safe,
                                  2 = failed uncovered *)


start = (n_ins, n_proc, n_dis, n_tx, n_rx, n_ant, 0);

(*  Including the deathif statements will aggregate each trapping
state into
    one of two states  *)

(* mapping code bombs on deathif states *)
(* comment out deathif states until mapping code upgraded *)
(* deathif f_mode = 1; *)
(* deathif f_mode = 2; *)


(*  Set up event transitions  *)

(*  Failure of INS  *)

if (m_ins >= 3) tranto m_ins = m_ins - 1 by m_ins*l_ins;
if (m_ins = 2) then
      tranto m_ins = m_ins - 1 by m_ins*c_ins_2*l_ins;
   tranto m_ins = m_ins - 1, f_mode = 2 by m_ins*(1 -
c_ins_2)*l_ins;
endif;
if (m_ins = 1) then
   tranto m_ins = m_ins - 1, f_mode = 1 by m_ins*c_ins_1*l_ins;
   tranto m_ins = m_ins - 1, f_mode = 2 by m_ins*(1 -
c_ins_1)*l_ins;
endif;

(*  Failure of ADS-B Processor  *)

if (m_proc >= 3) tranto m_proc = m_proc - 1 by m_proc*l_proc;
if (m_proc = 2) then
      tranto m_proc = m_proc - 1 by m_proc*c_proc_2*l_proc;
   tranto m_proc = m_proc - 1, f_mode = 2 by m_proc*(1 -
c_proc_2)*l_proc;
endif;
if (m_proc = 1) then
   tranto m_proc = m_proc - 1, f_mode = 1 by
m_proc*c_proc_1*l_proc;
   tranto m_proc = m_proc - 1, f_mode = 2 by m_proc*(1 -
c_proc_1)*l_proc;
endif;
```

```
(*  Failure of ADS-B Display  *)
if (m_dis >= 3) tranto m_dis = m_dis - 1 by m_dis*l_dis;
if (m_dis = 2) then
      tranto m_dis = m_dis - 1 by m_dis*c_dis_2*l_dis;
   tranto m_dis = m_dis - 1, f_mode = 2 by m_dis*(1 -
c_dis_2)*l_dis;
endif;
if (m_dis = 1) then
   tranto m_dis = m_dis - 1, f_mode = 1 by m_dis*c_dis_1*l_dis;
   tranto m_dis = m_dis - 1, f_mode = 2 by m_dis*(1 -
c_dis_1)*l_dis;
endif;

(* Failure of Modulator and Transmitter channel *)

if (m_tx = 1) then
   tranto m_tx = m_tx - 1, f_mode = 1 by m_tx*c_tx*l_tx;
   tranto m_tx = m_tx - 1, f_mode = 2 by m_tx*(1 - c_tx)*l_tx;
endif;

(* Failure of Receiver and Demodulator channel *)

if (m_rx = 1) then
   tranto m_rx = m_rx - 1, f_mode = 1 by m_rx*c_rx*l_rx;
   tranto m_rx = m_rx - 1, f_mode = 2 by m_rx*(1 - c_rx)*l_rx;
endif;

(*  Failure of Antenna  *)

if (m_ant = 1) then
   tranto m_ant = m_ant - 1, f_mode = 1 by m_ant*c_ant*l_ant;
   tranto m_ant = m_ant - 1, f_mode = 2 by m_ant*(1 -
c_ant)*l_ant;
endif;
```

Appendix F
Approach Aids Model—Delayed Repair

```
LIST = 3;
PRUNE = 0;

local_f  = 1/3000;   (* Localizer - Ground Track System *)
local_r  = 1/4;      (* MTTR - Localizer *)

gld_sl_f = 1/2000;   (* Glideslope - Descent Path System *)
gld_sl_r = 1/2;      (* MTTR - Glideslope *)
gld_sl_w = 1/12;        (* Mean Wait Time for Glideslope*)

o_mrk_f  = 1/2000;   (* Outer Marker *)
o_mrk_r  = 1/4;      (* MTTR - Outer Marker *)
o_mrk_w  = 1/48;        (* Mean Wait Time for Outer Marker *)

m_mrk_f  = 1/2000;   (* Middle Marker *)
m_mrk_r  = 1/4;      (* MTTR - Middle Marker *)
m_mrk_w  = 1/48;        (* Mean Wait Time for Middle Marker *)

app_lt_f = 1/1000;   (* Approach Lights *)
app_lt_r = 1/2;      (* MTTR - Approach Lights *)
app_lt_w = 1/72;        (* Mean Wait Time for Approach Lights *)

thr_lt_f = 1/1000;   (* Threshold Lights *)
thr_lt_r = 1/2;      (* MTTR - Threshold Lights *)
thr_lt_w = 1/72;        (* Mean Wait Time for Threshold Lights *)

SPACE = (local: 0..1,
    gld_sl: 0..1, gld_sl_wait: 0..2,
    o_mrk: 0..1,  o_mrk_wait: 0..2,
    m_mrk: 0..1,  m_mrk_wait: 0..2,
    app_lt: 0..1, app_lt_wait: 0..2,
    thr_lt: 0..1, thr_lt_wait: 0..2);
(* o_mrk_wait = 0 - no failure; = 1 - failure *)

START = (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0); (* o_mrk = 0 - no
failure *)

(* ------------------------------------------------------------ *)
IF (o_mrk_wait < 2 and m_mrk_wait < 2 and thr_lt_wait < 2
   and app_lt_wait < 2 and gld_sl_wait < 2) then

IF local > 0 TRANTO local = local - 1 BY local_f;
IF local < 1 TRANTO local = local + 1 BY local_r;

endif;
(* ------------------------------------------------------------ *)

IF (o_mrk_wait < 2 and m_mrk_wait < 2 and thr_lt_wait < 2 and
app_lt_wait < 2) then
```

```
IF gld_sl_wait = 0 then
   if gld_sl > 0 TRANTO gld_sl_wait = 1, gld_sl = gld_sl - 1 BY
gld_sl_f;
   endif;
IF gld_sl_wait = 1 then
   if gld_sl = 0 TRANTO gld_sl_wait = 2 BY gld_sl_w;
   endif;
IF gld_sl_wait = 2  TRANTO gld_sl_wait = 0, gld_sl = gld_sl + 1
BY gld_sl_r;
endif;
(* ---------------------------------------------------------- *)

IF (gld_sl_wait < 2 and m_mrk_wait < 2 and thr_lt_wait < 2 and
app_lt_wait < 2) then

IF o_mrk_wait = 0 then
   if o_mrk > 0 TRANTO o_mrk_wait = 1, o_mrk = o_mrk - 1 BY
o_mrk_f;
   endif;
(* endif; *)
IF o_mrk_wait = 1 then
   if o_mrk = 0 TRANTO o_mrk_wait = 2 BY o_mrk_w;
   endif;
IF o_mrk_wait = 2  TRANTO o_mrk_wait = 0, o_mrk = o_mrk + 1 BY
o_mrk_r;

endif;

(* ---------------------------------------------------------- *)

IF (gld_sl_wait < 2 and o_mrk_wait < 2 and thr_lt_wait < 2 and
app_lt_wait < 2) then

IF m_mrk_wait = 0 then
   if m_mrk > 0 TRANTO m_mrk_wait = 1, m_mrk = m_mrk - 1 BY
m_mrk_f;
   endif;
IF m_mrk_wait = 1 then
   if m_mrk = 0 TRANTO m_mrk_wait = 2 BY m_mrk_w;
   endif;
IF m_mrk_wait = 2  TRANTO m_mrk_wait = 0, m_mrk = m_mrk + 1 BY
m_mrk_r;
endif;
(* ------------------------------------------------------------
*)
IF (gld_sl_wait < 2 and o_mrk_wait < 2 and thr_lt_wait < 2 and
m_mrk_wait < 2) then

IF app_lt_wait = 0 then
   if app_lt > 0 TRANTO app_lt_wait = 1, app_lt = app_lt - 1 BY
app_lt_f;
   endif;
IF app_lt_wait = 1 then
if app_lt = 0 TRANTO app_lt_wait = 2 BY app_lt_w;
   endif;
```

```
IF app_lt_wait = 2  TRANTO app_lt_wait = 0, app_lt = app_lt + 1
BY app_lt_r;
endif;
(* ---------------------------------------------------------- *)
IF (gld_sl_wait < 2 and o_mrk_wait < 2 and app_lt_wait < 2 and
m_mrk_wait < 2) then

IF thr_lt_wait = 0 then
   if thr_lt > 0 TRANTO thr_lt_wait = 1, thr_lt = thr_lt - 1 BY
thr_lt_f;
   endif;
IF thr_lt_wait = 1 then
   if thr_lt = 0 TRANTO thr_lt_wait = 2 BY app_lt_w;
   endif;
IF thr_lt_wait = 2  TRANTO thr_lt_wait = 0, thr_lt = thr_lt + 1
BY thr_lt_r;
endif;
```

Appendix G

Approach Aids Model—Immediate Repair

```
LIST = 3;
PRUNE = 0;
local_f  = 1/3000;    (* Localizer - Ground Track System *)
local_r  = 1/4;       (* MTTR - Localizer *)
gld_sl_f = 1/2000;    (* Glideslope - Descent Path System *)
gld_sl_r = 1/2;       (* MTTR - Glideslope *)
o_mrk_f  = 1/2000;    (* Outer Marker *)
o_mrk_r  = 1/4;       (* MTTR - Outer Marker *)
m_mrk_f  = 1/2000;    (* Middle Marker *)
m_mrk_r  = 1/4;       (* MTTR - Middle Marker *)
app_lt_f = 1/1000;    (* Approach Lights *)
app_lt_r = 1/2;       (* MTTR - Approach Lights *)
thr_lt_f = 1/1000;    (* Threshold Lights *)
thr_lt_r = 1/2;       (* MTTR - Threshold Lights *)

SPACE = (local: 0..1, gld_sl: 0..1, o_mrk: 0..1, m_mrk: 0..1,
app_lt: 0..1, thr_lt: 0..1);

START = (1, 1, 1, 1, 1, 1);

IF local > 0 TRANTO local = local - 1 BY local_f;
IF local < 1 TRANTO local = local + 1 BY local_r;

IF gld_sl > 0 TRANTO gld_sl = gld_sl - 1 BY gld_sl_f;
IF gld_sl < 1 TRANTO gld_sl = gld_sl + 1 BY gld_sl_r;

IF o_mrk > 0 TRANTO o_mrk = o_mrk - 1 BY o_mrk_f;
IF o_mrk < 1 TRANTO o_mrk = o_mrk + 1 BY o_mrk_r;

IF m_mrk > 0 TRANTO m_mrk = m_mrk - 1 BY m_mrk_f;
IF m_mrk < 1 TRANTO m_mrk = m_mrk + 1 BY m_mrk_r;

IF app_lt > 0 TRANTO app_lt = app_lt - 1 BY app_lt_f;
IF app_lt < 1 TRANTO app_lt = app_lt + 1 BY app_lt_r;

IF thr_lt > 0 TRANTO thr_lt = thr_lt - 1 BY thr_lt_f;
IF thr_lt < 1 TRANTO thr_lt = thr_lt + 1 BY thr_lt_r;
```

Appendix H
WAAS-GPS Receiver Model

```
(*  ASSIST Input File to Generate       *)
(*  WAAS GPS Receiver SURE Input File   *)

(*  Number of Redundant Components of Each Type  *)

n_ant = 2;    (* GPS Antennas *)
n_rx = 3;     (* GPS Receivers *)
n_proc = 2;   (* WAAS Processors *)
n_dis = 2;    (* WAAS Displays *)

(*  Failure Rates  *)
l_ant =  1.e-6;   (* GPS Antennas *)
l_rx =   3.e-5;   (* GPS Receivers *)
l_proc = 1.e-5;   (* WAAS Processor *)
l_dis =  2.e-5;   (* WAAS Displays *)

(*  Coverage Probabilities  *)
c_ant_2 =  1.00;   (* GPS Antennas, two on-line *)
c_ant_1 =  1.00;   (* GPS Antennas, one on-line *)
c_rx_2 =   0.99;   (* GPS Receivers, two on-line *)
c_rx_1 =   0.95;   (* GPS Receivers, one on-line *)
c_proc_2 = 0.99;   (* WAAS Processors, two on-line *)
c_proc_1 = 0.95;   (* WAAS Processors, one on-line *)
c_dis_2 =  0.999;  (* WAAS Displays, two on-line *)
c_dis_1 =  0.99;   (* WAAS Displays, one on-line *)

(*  Other Parameters  *)

LIST = 3;                    (* Needed for the .mod file *)
n_modes = 2;                 (* Number of system failure modes
which
                                will be differentiated in model *)


space = (m_ant: 0..n_ant,      (* Number of on-line Antennas *)
         m_rx: 0..n_rx,        (* Number of on-line GPS Receivers
*)
         m_proc: 0..n_proc,    (* Number of on-line WAAS Proces-
sors *)
         m_dis: 0..n_dis,      (* Number of on-line WAAS Displays
*)
         f_mode: 0..n_modes); (* Flag indicating system failure
mode
                                   0 = operational state,
                                   1 = failed safe,
                                   2 = failed uncovered *)


start = (n_ant, n_rx, n_proc, n_dis, 0);
```

```
(*  Including the deathif statements will aggregate each trapping
state into
    one of two states  *)

(* deathif f_mode = 1; *)
(* deathif f_mode = 2; *)


(*  Set up event transitions  *)

(*  Failure of Antenna  *)

if (m_ant >= 3) tranto m_ant = m_ant - 1 by m_ant*l_ant;
if (m_ant = 2) then
      tranto m_ant = m_ant - 1 by m_ant*c_ant_2*l_ant;
   tranto m_ant = m_ant - 1, f_mode = 2 by m_ant*(1 -
c_ant_2)*l_ant;
endif;
if (m_ant = 1) then
   tranto m_ant = m_ant - 1, f_mode = 1 by m_ant*c_ant_1*l_ant;
   tranto m_ant = m_ant - 1, f_mode = 2 by m_ant*(1 -
c_ant_1)*l_ant;
endif;

(*  Failure of GPS Receiver  *)

if (m_rx >= 3) tranto m_rx = m_rx - 1 by m_rx*l_rx;
if (m_rx = 2) then
      tranto m_rx = m_rx - 1 by m_rx*c_rx_2*l_rx;
   tranto m_rx = m_rx - 1, f_mode = 2 by m_rx*(1 - c_rx_2)*l_rx;
endif;
if (m_rx = 1) then
   tranto m_rx = m_rx - 1, f_mode = 1 by m_rx*c_rx_1*l_rx;
   tranto m_rx = m_rx - 1, f_mode = 2 by m_rx*(1 - c_rx_1)*l_rx;
endif;

(*  Failure of WAAS Processor  *)

if (m_proc >= 3) tranto m_proc = m_proc - 1 by m_proc*l_proc;
if (m_proc = 2) then
      tranto m_proc = m_proc - 1 by m_proc*c_proc_2*l_proc;
   tranto m_proc = m_proc - 1, f_mode = 2 by m_proc*(1 -
c_proc_2)*l_proc;
endif;
if (m_proc = 1) then
   tranto m_proc = m_proc - 1, f_mode = 1 by
m_proc*c_proc_1*l_proc;
   tranto m_proc = m_proc - 1, f_mode = 2 by m_proc*(1 -
c_proc_1)*l_proc;
endif;

(*  Failure of WAAS Display  *)

if (m_dis >= 3) tranto m_dis = m_dis - 1 by m_dis*l_dis;
if (m_dis = 2) then
      tranto m_dis = m_dis - 1 by m_dis*c_dis_2*l_dis;
   tranto m_dis = m_dis - 1, f_mode = 2 by m_dis*(1 -
c_dis_2)*l_dis;
endif;
if (m_dis = 1) then
   tranto m_dis = m_dis - 1, f_mode = 1 by m_dis*c_dis_1*l_dis;
   tranto m_dis = m_dis - 1, f_mode = 2 by m_dis*(1 -
c_dis_1)*l_dis;
endif;
```

Appendix I
GPS Surveillance Model—No Spare Satellite

```
(* Needed for the .mod file *)
LIST = 3;
PRUNE = 0;
(* How many of each item there are *)
REDUNDANT = 1;
(* Number of failure states *)
STATES = 2;
(* Failure Rates *)
FAIL1 = 2.273E-4;
FAIL2 = 3.84E-5;
(* Recovery rates *)
RECOVER1 = 1.212;
RECOVER2 = 9.144E-4;
(* 1 means the repairs are done in parallel, 0 means in serries
*)
PARALLEL = 1;

(* Starting Info *)
SPACE = (WORKING: 0..REDUNDANT, ITEM : ARRAY[1..STATES] OF
0..REDUNDANT);
START = (REDUNDANT, STATES OF 0);

(* Set up the failure rates *)
IF (WORKING > 0) THEN
   FOR I = 1,STATES
      TRANTO WORKING = WORKING - 1, ITEM[I] = ITEM[I] + 1 BY
WORKING * FAIL^I;
   ENDFOR;
ENDIF;

FOR I = 1,STATES
   IF (ITEM[I] > 0) THEN
      IF (PARALLEL = 1) THEN
         TRANTO WORKING = WORKING + 1, ITEM[I] = ITEM[I] - 1 BY
ITEM[I]*RECOVER^I;
      ELSE
         TRANTO WORKING = WORKING + 1, ITEM[I] = ITEM[I] - 1 BY
RECOVER^I;
      ENDIF;
   ENDIF;
ENDFOR;
```

Appendix J

GPS Surveillance Model—Global Spare Satellite

```
(* Copy Time statement to outfile for PAWS *)
"TIME = 1 TO* 1000000 BY 10;"
(* Needed for the .mod file *)
LIST = 3;
(* Number of primary geo satellites providing local waas coverage
*)
PRIMARY = 1;
(* Minimum number of primary geo satellites required *)
PRI_MIN = 1;
(* Number of secondary geo satellites global coverage elsewhere
*)
SECONDARY = 3;
(* Minimum number of secondary geo satellites required *)
SEC_MIN = 3;
(* Number of reserve geo satellites used as spare *)
RESERVE =1;
(* Number of failure states *)
STATES = 2;
(* Failure Rates *)
FAIL1 = 2.273E-4;
FAIL2 = 3.84E-5;
(* Failure rates are identical *)
(* Assist requiring space vector element to have individual
rate*)
PF1=FAIL1;
PF2=FAIL2;
SF1=FAIL1;
SF2=FAIL2;
RF1=FAIL1;
RF2=FAIL2;
(* Recovery rates *)
RECOVER1 = 1.212;
RECOVER2 = 9.144E-4;
(* Recovery rates are identical *)
(* Assist requiring space vector element to have individual
rate*)
PR1=RECOVER1;
PR2=RECOVER2;
SR1=RECOVER1;
SR2=RECOVER2;
RR1=RECOVER1;
RR2=RECOVER2;
(* Repositioning rate *)
REPOSITION =  3.333E-2;
M = REPOSITION;
(* 1 means the repairs are done in parallel, 0 means in series *)
PARALLEL = 1;

(* Starting Info *)
(* State definition:                     *)
(* # of primary geos operational         *)
(* # of primary geos in failure mode 1   *)
(* # of primary geos in failure mode 2   *)
(* # of secondary geos operational       *)
(* # of secondary geos in failure mode 1 *)
(* # of secondary geos in failure mode 2 *)
(* # of reserve geos operational         *)
(* # of reserve geos in failure mode 1   *)
(* # of reserve geos in failure mode 2   *)
N = STATES;
P = PRIMARY;
S = SECONDARY;
R = RESERVE;
SPACE = (PRI: 0..P, PFAIL: ARRAY[1..N] OF 0..P, SEC: 0..S, SFAIL:
ARRAY[1..N] OF 0..S, RES: 0..R, RFAIL: ARRAY[1..N] OF 0..R);
START = (PRIMARY, 0, 0, SECONDARY, 0, 0, RESERVE, 0, 0);

(* Set up the failure rates *)
IF (PRI > 0) THEN
   FOR I = 1,STATES
      TRANTO PRI = PRI - 1, PFAIL[I] = PFAIL[I] + 1 BY PRI *
PF^I;
   ENDFOR;
ENDIF;

IF (SEC > 0) THEN
   FOR I = 1,STATES
      TRANTO SEC = SEC - 1, SFAIL[I] = SFAIL[I] + 1 BY SEC *
SF^I;
   ENDFOR;
ENDIF;

IF (RES > 0) THEN
   FOR I = 1,STATES
      TRANTO RES = RES - 1, RFAIL[I] = RFAIL[I] + 1 BY RES *
RF^I;
   ENDFOR;
ENDIF;

(* Set up the recovery rates *)
FOR I = 1,STATES
   IF (PFAIL[I] > 0) THEN
      IF (PARALLEL = 1) THEN
         TRANTO PRI = PRI + 1, PFAIL[I] = PFAIL[I] - 1 BY
PFAIL[I]*PR^I;
      ELSE
         TRANTO PRI = PRI + 1, PFAIL[I] = PFAIL[I] - 1 BY PR^I;
      ENDIF;
   ENDIF;
ENDFOR;

FOR I = 1,STATES
   IF (SFAIL[I] > 0) THEN
      IF (PARALLEL = 1) THEN
         TRANTO SEC = SEC + 1, SFAIL[I] = SFAIL[I] - 1 BY
SFAIL[I]*SR^I;
```

```
      ELSE
         TRANTO SEC = SEC + 1, SFAIL[I] = SFAIL[I] - 1 BY SR^I;
      ENDIF;
   ENDIF;
ENDFOR;

FOR I = 1,STATES
   IF (RFAIL[I] > 0) THEN
      IF (PARALLEL = 1) THEN
         TRANTO RES = RES + 1, RFAIL[I] = RFAIL[I] - 1 BY
RFAIL[I]*RR^I;
      ELSE
         TRANTO RES = RES + 1, RFAIL[I] = RFAIL[I] - 1 BY RR^I;
      ENDIF;
   ENDIF;
ENDFOR;

(* Set up spare transition *)
IF (RES > 0) THEN
   FOR I = 1,STATES

      IF (PRI < PRI_MIN AND PFAIL[I] > 0) THEN
         TRANTO PRI=PRI+1, PFAIL[I]=PFAIL[I]-1, RES=RES-1,
RFAIL[I]=RFAIL[I]+1 BY PFAIL[I] * M / (P-PRI + S-SEC);
      ENDIF;

      IF (SEC < SEC_MIN AND SFAIL[I] > 0) THEN
         TRANTO SEC=SEC+1, SFAIL[I]=SFAIL[I]-1, RES=RES-1,
RFAIL[I]=RFAIL[I]+1 BY SFAIL[I] * M / (P-PRI + S-SEC);
      ENDIF;

   ENDFOR;
ENDIF;
```

REPORT DOCUMENTATION PAGE	*Form Approved* *OPM No.0704-0188*

1. AGENCY USE ONLY *(Leave Blank)*

2. REPORT DATE

August 1999

3. REPORT TYPE AND DATES COVERED

Contractor Report

4. TITLE AND SUBTITLE

A System for Integrated Reliability and Safety Analyses

5. FUNDING NUMBERS

C NAS2-14361

WU 536-16-11-01

6. AUTHOR(S)

Peter Kostiuk, Gerald Shapiro, Dave Hanson, Stephan Kolitz, Frank Leong, Gene Rosch, Marc Coumeri, Peter Scheidler, Jr., and Charles Bonesteel

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Logistics Management Institute
2000 Corporate Ridge
McLean, VA 22102-7805

8. PERFORMING ORGANIZATION REPORT NUMBER

NS805S1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681-0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA/CR-1999-209548

11. SUPPLEMENTARY NOTES

Langley Technical Monitor. Robert Yackovetsky
Final Report
P. Kostiuk, G. Shapiro (LMI), D. Hanson, S. Kolitz, F. Leong, G. Rosch, M. Coumeri, P. Scheidler, Jr. (Draper Lab.), and C. Bonesteel (Chava Group)

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified-Unlimited
Subject Category 01
Availability: NASA CASI (301) 621-0390
Distribution: Nonstandard

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

We present an integrated reliability and aviation safety analysis tool. The reliability models for selected infrastructure components of the air traffic control system are described. The results of this model are used to evaluate the likelihood of seeing outcomes predicted by simulations with failures injected. We discuss the design of the simulation model, and the user interface to the integrated toolset.

14. SUBJECT TERMS

ASAC, Aviation, Safety, Reliability, NAS

15. NUMBER OF PAGES

82

16. PRICE CODE

A05

17. SECURITY CLASSIFICATION OF REPORT

Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE

Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT

20. LIMITATION OF ABSTRACT

UL